

FM 3-19.50

Police Intelligence Operations

July 2006

DISTRIBUTION RESTRICTION: Approved for public release, distribution is unlimited.

Headquarters, Department of the Army

**This publication is available at
Army Knowledge Online <<https://www.us.army.mil>>
and General Dennis J. Reimer Training and Doctrine
Digital Library at <<http://www.train.army.mil>>.**

Police Intelligence Operations

Contents

	Page
PREFACE	iv
Chapter 1 INTRODUCTION	1-1
Background	1-1
Role of Police Intelligence Operations	1-1
Development of an Effective Police Intelligence Operations Network	1-6
Common Police Intelligence Operations Definitions	1-7
Application of Police Intelligence Operations	1-7
Army Law Enforcement Policy	1-8
Chapter 2 LEGAL DOCUMENTS AND CONSIDERATIONS	2-1
<i>Executive Order 12333</i>	2-1
<i>Department of Defense Directive 5200.27</i>	2-2
<i>Army Regulation 190-45</i>	2-3
<i>Army Regulation 195-1</i>	2-4
<i>Army Regulation 195-2</i>	2-4
<i>Army Regulation 380-13</i>	2-4
<i>Army Regulation 381-10</i>	2-4
<i>Army Regulation 525-13</i>	2-5
<i>Criminal Investigations Division Regulation 195-1</i>	2-6
<i>Department of Defense Directive 2000.12 and Department of Defense Instruction 2000.16</i>	2-7
<i>USA Patriot Act</i>	2-7
Status of Forces Agreements and International Law	2-8
Chapter 3 POLICE INTELLIGENCE OPERATIONS AS EMERGING DOCTRINE	3-1
Effective Police Intelligence Operations Development	3-1
Command Staff Process	3-1
Police Information Collection Process	3-7
Reconnaissance and Surveillance	3-9

Chapter 4	THE CRIMINAL INTELLIGENCE PROCESS IN SUPPORT OF POLICE INTELLIGENCE OPERATIONS.....	4-1
	Criminal Intelligence Process	4-1
	Databases.....	4-7
	Centralized Criminal Intelligence Analytical Support Element and Database	4-7
	Police Records Management.....	4-9
Chapter 5	POLICE INTELLIGENCE OPERATIONS IN URBAN OPERATIONS	5-1
	Urban Threats	5-1
	Army Law Enforcement in Urban Operations	5-3
	Intelligence Preparation of the Battlefield in Urban Operations.....	5-3
	Urban Intelligence, Surveillance, and Reconnaissance	5-4
Chapter 6	POLICE INTELLIGENCE OPERATIONS ON INSTALLATIONS.....	6-1
	Responsibilities of the Installation Management Agency	6-1
	Authority to Conduct Police Intelligence Operations	6-1
	Management of Police Intelligence Operations on Installations	6-2
Chapter 7	POLICE INTELLIGENCE OPERATIONS NETWORKING	7-1
	Nontactical Networks	7-1
	Tactical Networks.....	7-2
	Defining Network Participants.....	7-2
	Forums and Threat Working Groups	7-4
Appendix A	INTEGRATING POLICE INTELLIGENCE OPERATIONS PLANNING IN THE MILITARY DECISION-MAKING PROCESS	A-1
Appendix B	SAMPLE CRIMINAL INTELLIGENCE PRODUCTS	B-1
Appendix C	SAMPLE POLICE INTELLIGENCE OPERATIONS CHEKLIST	C-1
Appendix D	TACTICAL QUESTIONING.....	D-1
Appendix E	QUESTION TO ASK DETAINEES.....	E-1
Appendix F	DEBRIEFING AND/OR AFTER-ACTION REVIEWS.....	F-1
Appendix G	SOURCES	G-1
	GLOSSARY	Glossary-1
	REFERENCES.....	References-1
	INDEX	Index-1

Figures

Figure 1-1. Information Sharing Through PIO	1-8
Figure 3-1. Command Staff Process	3-2
Figure 3-2. Police Information and CRIMINT Products Input into the Intelligence Process.....	3-3
Figure 3-3. Police Information Collection Process.....	3-6
Figure 3-4. SALUTE Report.....	3-9
Figure 4-1. CRIMINT Process.....	4-2

Figure 4-2. Police Intelligence Process Model.....	4-5
Figure 4-3. Sample of Planning for and Execution of PIO Functions.....	4-8
Figure 6-1. US Army Installation Threat and Crime Model	6-3
Figure 7-1. Nontactical PIO Network.....	7-2
Figure 7-2. Tactical PIO Network	7-3
Figure 7-3. Organizational Chart.....	7-4
Figure A-1. MDMP.....	A-1
Figure A-2. PIO Criminal Dimension and the MDMP	A-5
Figure B-1. BOLO Alert	B-2
Figure B-2. Sample of an Open-Source Intelligence Daily Report.....	B-2
Figure B-3. Sample of a US Postal Inspection Wanted Poster.....	B-6
Figure B-4. Sample of an FBI Wanted Poster.....	B-7
Figure B-5. Link Analysis Chart.....	B-8
Figure C-1. Sample PIO Checklist	C-1

Tables

Table 1-1. Primary Intelligence Tasks.....	1-3
--	-----

Preface

Field Manual (FM) 3-19.50 is a new FM and is the Military Police Corps' manual for police intelligence operations (PIO) doctrine. It describes—

- The fundamentals of PIO.
- The legal documents and considerations affiliated with PIO.
- The PIO process.
- The relationship of PIO to the Army's intelligence process.
- The introduction of police and prison structures, organized crime, legal systems, investigations, crime-conducive conditions, and enforcement mechanisms and gaps (POLICE)—a tool to assess the criminal dimension and its influence on effects-based operations (EBO).
- PIO in urban operations (UO) and on installations.
- The establishment of PIO networks and associated forums and fusion cells to affect gathering police information and criminal intelligence (CRIMINT).

This manual is targeted specifically for the military police battalion staff, the Criminal Investigation Division Command (CID), the director of emergency services (DES), the provost marshal (PM), other military police leaders, and Army law enforcement (ALE) personnel who are responsible for managing and executing the PIO function. ALE includes military police and Department of the Army (DA) police and security guards.

This publication applies to the Active Army, the Army National Guard (ARNG)/the Army National Guard of the United States, and the United States Army Reserve.

The proponent of this publication is the United States Army Training and Doctrine Command (TRADOC). Send comments and recommendations on *DA Form 2028 (Recommended Changes to Publications and Blank Forms)* directly to Commandant, United States Army Military Police School (USAMPS), ATTN: ATSJ-MP-TD, 401 MANSCEN Loop, Suite 2060, Fort Leonard Wood, Missouri 65473-8926.

Unless stated otherwise, masculine nouns or pronouns do not refer exclusively to men.

Chapter 1

Introduction

Over the last several years, the senior military police leadership has recognized the value and role that PIO play in bridging the information gap in a commander's situational understanding and force protection (FP) programs. With the events of 11 September 2001 and the initiation of offensive combat actions in Operation Iraqi Freedom (OIF) and Operation Enduring Freedom (OEF), emerging doctrine, and the expanding role the US military is playing in "nation building," there has been a renewed interest in police intelligence efforts and support to installation and maneuver commanders. The military police component addresses this interest through the PIO function, which includes a review of the environment in a holistic approach, analyzing both the criminal threat and the capabilities of existing law enforcement agencies. This review is an assessment of the criminal dimension when considering the civil environment in mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC).

BACKGROUND

1-1. PIO are a military police function that supports, enhances, and contributes to a commander's situational understanding and battlefield visualization and FP programs by portraying the relevant criminal threat and friendly information, which may affect his operational and tactical environment. They are a function (consisting of systems, processes, and tools) that capitalizes on military police capabilities to analyze police information and develop criminal intelligence through the integration and employment of ALE assets and other police organizations. Like the military intelligence (MI) officer (intelligence staff officer [S2] and assistant chief of staff, intelligence [G2]) uses the intelligence preparation of the battlefield (IPB) process to analyze the threat and the environment continuously in a specific geographical area, military police leaders use PIO to assist the G2 and to collect, organize, and analyze police information continuously as part of the IPB process. As described in this and later chapters, PIO contribute to the IPB; they are not a substitute for the IPB.

1-2. *Department of Defense Directives (DODDs) 2000.12 and 2000.16* direct and give commanders the authority to task subordinate organizations to gather, analyze, and disseminate terrorism threat information. *Army Regulation (AR) 525-13* tasks commanders similarly when collecting and analyzing criminal threat information. It is under the authority of these legal instruments and those outlined in [Chapter 2](#) that the function of PIO is executed and managed. The purpose of PIO is twofold:

- It provides lethal (kinetic) or nonlethal (nonkinetic) targeting to the commander and PM with CRIMINT, targeting criminal threat systems and elements that threaten a mission or operation and the safety and security of the installation and its personnel and resources.
- It provides nonlethal or nonkinetic information to the commander and PM with a situational understanding of the capabilities and challenges of the criminal justice system within a given area of operation (AO).

ROLE OF POLICE INTELLIGENCE OPERATIONS

1-3. Due to the complexity of the environment, units often need to respond to multiple threats. The commander must understand how current and potential threat systems (along with the system of friendly agencies) organize, equip, and employ their forces.

1-4. In tactical environments, PIO will occur as a routine part of conducting other military police missions, but they can also serve as a primary function in order to support intelligence-driven operations. During offensive and defensive operations, PIO serve to identify systems (criminal or police) within the environment in order to indicate the conditions needed to establish stability. As operations become more protracted and conventional, threat levels are reduced from a traditional military threat to a more asymmetric threat, where the environment between criminal, terrorist, and insurgent activities normally associated with stability operations becomes blurred. PIO serve as a contributing function, which enables the S2/G2 to accurately articulate to the commander the environment and those who oppose stability. This is especially true during stability operations where the role of the military police focuses on developing a country's ability to protect its communities and enforce the laws. When PIO are planned for and conducted in stability operations, they foster the success of the operation and meet the commander's desired outcome. In nontactical environments, PIO provide essential products and services in support of military operations. In particular, PIO can work to reduce threats against Army installations; provide threat intelligence for in-transit security; and focus the development and implementation of threat countermeasures to safeguard Army personnel, material, and information. Regardless of the operational environment (OE), PIO help bridge the information gap between what a commander does and does not know. PIO provide direct support to the MI cycle and provide the most reliable information through developing effective PIO networks.

BRIDGING THE INFORMATION GAP

1-5. When the S2/G2 identifies a gap in the commander's knowledge of the threat and the current threat situation, that gap may be included as priority intelligence requirements (PIR) or selected as indications and warnings (I&W). The S2/G2 will then develop a collection plan to assist the commander in filling this information gap. Part of the commander's collection strategy is to select the best collection asset available to cover each information requirement. After a thorough analysis (which includes availability, capability, and performance history), the collection manager identifies which collection asset can best be used. When the military police, CID, and DA police and security guards—henceforth referred to as ALE—are tasked with the police information collection mission, they are provided with specific guidelines and a prioritized collection requirement (see *FM 34-2*). In the continental United States (CONUS), effective PIO can provide installation commanders with situational understanding and address any information gaps to ensure that threat assessments are both valid and reliable. According to *DODD 5200.27*, "where collection activities are authorized to meet an essential requirement for information, maximum reliance shall be placed upon domestic civilian investigative agencies, federal, state, and local." PIO emphasize connectivity between installation law enforcement and civilian domestic agencies.

1-6. The above paragraph discusses the direct tasking of ALE assets in support of the PIO function when an information gap has been identified. It must be recognized that combat service support patrols and presence patrols conducted by infantry and armor units may provide input to the police collection effort by virtue of their presence at a given location and time.

SUPPORTING MILITARY INTELLIGENCE WITH POLICE INTELLIGENCE OPERATIONS

1-7. Within the intelligence warfighting function (WFF), personnel and organizations conduct four primary intelligence tasks that facilitate the commander's visualization and understanding of the threat and the battlespace (see *FM 2-0*). These tasks are as follows:

- Support situational understanding.
- Support strategic responsiveness.
- Conduct intelligence, surveillance, and reconnaissance (ISR).
- Provide intelligence support to effects.

1-8. These tasks are interactive and often take place simultaneously. *Table 1-1* shows these tasks tailored to the commander's needs.

1-9. It is within the critical intelligence task "support situational understanding" that PIO best support the MI cycle. PIO are essential to this task, particularly where asymmetric threats (criminals, terrorists, and

insurgents) threaten the security of US forces and military operations. UO are an example of where there may be a high volume of asymmetric threats and where the demand for directed police information collection is required and appropriate. Emerging with equal importance is the support PIO provide to intelligence efforts concerning effects. As the role of the military focuses on developing a country's infrastructure, the military police staff will serve as the subject matter expert on building an effective law enforcement agency within that country's criminal justice system. This will require an analysis of current capabilities and the necessary actions needed to stand up or improve an agency.

1-10. Support to situational understanding centers on providing military information and intelligence to the commander, which facilitates his understanding of the enemy and the environment. This task supports the command's ability to make sound decisions.

Table 1-1. Primary Intelligence Tasks

<i>Intelligence Tasks</i>	<i>Commander's Focus</i>	<i>Commander's Decisions</i>
Support situational understanding. • Perform IPB. • Perform situation development. • Provide intelligence support to FP. • Conduct PIO.	Plan a mission. Execute the operation. Secure the force.	Which course of action (COA) should be implemented? Which enemy actions are expected?
Support strategic responsiveness. • Interpret I&W. • Ensure intelligence readiness. • Conduct area studies of foreign countries. • Support sensitive site exploitation.	Orient on contingencies.	Should the unit's level of readiness be increased? Should the operation plan (OPLAN) be implemented?
Conduct ISR. • Perform intelligence synchronization. • Perform ISR integration. • Conduct tactical reconnaissance. • Conduct surveillance.	Plan, prepare, execute, and assess the mission.	Which decision points (DPs), high-payoff targets (HPTs), and so forth are linked to enemy actions? Are assets available and in position to collect on the DPs, HPTs, and so forth? Have assets been repositioned for the contingency mission?
Provide intelligence support to effects. • Provide intelligence support to targeting. • Provide intelligence support to host nation (HN) organizations. • Provide intelligence support to combat assessment.	Destroy, suppress, or neutralize targets. Reposition intelligence or attack assets.	Is fire (lethal or nonlethal) and maneuver effective? Should the same targets be refired upon?

Perform Intelligence Preparation of the Battlefield

1-11. The S2/G2 is the staff proponent for IPB. There is only one IPB performed in each headquarters; this IPB includes the input received from all affected staff cells. During the IPB process, the S2/G2 uses all available databases and intelligence sources and/or products (such as the analysis control element [ACE] and other joint, interagency, and multinational agencies and related MI disciplines) to analyze the threat and the environment. During the IPB process, the military police planner provides an in-depth assessment of the criminal dimension using the acronym POLICE (see [paragraph 1-16](#)). The military police planner (in conjunction with the civil affairs officer [S5] and/or assistant chief of staff, civil affairs [G5]), supports this process by providing the S2/G2 with collected police, criminal, and combat information that can directly or indirectly affect the commander's lines of operations. By conducting a thorough review of existing police capabilities and known criminal activities, the military police planner identifies potential risks in each COA developed and significantly contributes to the success of the MI effort. In addition to the combat information, the PIO function provides additional information on possible criminal threats and COAs that may support the IPB process and that can be used by the commander to upgrade the FP posture.

Perform Situation Development

1-12. Situation development is a process for analyzing information and producing current MI about the enemy and the environment during operations. This process helps the MI officer recognize and interpret the indicators of enemy intentions, objectives, combat effectiveness, and potential enemy courses of action (ECOAs). This task allows the S2 to identify information gaps quickly. The military police representative to the G2 reviews raw data and intelligence to determine if any patterns, trends and associations exist within the criminal dimension. When analyzing the environment, the military police representative looks for patterns and trends that indicate the environment as crime-conducive or becoming crime-conducive. For example, a surge in kidnappings, the bombing of police stations, or simple graffiti represents patterns or trends of an organized effort to develop a sanctuary for criminal activity. The military police representative will then compare this information with previous activity in other areas to determine the group and the organized system.

Perform Intelligence Support to Force Protection

1-13. Intelligence support to FP consists of monitoring and reporting the activities, intentions, and capabilities of adversarial groups and determining their possible COA. Detecting the adversary's methods in today's OE requires a higher level of situational understanding. This type of threat drives the need for predictive intelligence based on an analysis of focused information from intelligence, law enforcement, and security activities.

Conduct Police Intelligence Operations

1-14. PIO provide situational understanding and visualization across the OE and are essential to the success of Army protective programs. When PIO are conducted in coordination with other law enforcement, security, and intelligence organizations, they can expand visualization beyond the AO to include the entire area of interest (AI). PIO consist of the staff's actions and processes the police information collection process (described in [Chapter 3](#)), and the CRIMINT process (described in [Chapter 4](#)), all of which input and result in the development of police intelligence products.

1-15. PIO play another important role in situational understanding through their review of the criminal dimension. (Criminal dimension planning considerations are included under the discussion of the military decision-making process [MDMP] in [Appendix A](#).) Often, in stability operations, the nature of the operation becomes more criminal and begins to influence friendly lines of operation, or the campaign plan. Because of this influence, it is necessary for military police planners to assess the presence of criminal aspects during major combat operations to help set the conditions of stability operations.

1-16. A tool that military police planners can use to assess the criminal dimension is POLICE. The components of POLICE can be useful in the assigning of tasks based on the desired effects (see [Appendix A](#)). Although useful throughout PIO, the criticality of using POLICE to analyze the criminal dimension before deployment cannot be overstated, especially for stability operations follow-on missions. The "P" in POLICE tells military police planners what police and prison structures exist. It will answer important questions such as the following:

- Is the indigenous police force corrupt?
- How is the indigenous police force received by the community?
- Can the indigenous police force be relied on as an asset to assist US and joint forces?
- What equipment, communications, and other capabilities does the indigenous police force have if it is reliable?
- How many prison structures exist within the AO and are they operational?
- How many police stations exist in the AO and are they operational?

Note: This list is not intended to be all-inclusive, but rather to act as a starting point.

1-17. The "O" in POLICE indicates the presence of organized crime and its purpose, such as to collect funding for insurgents or terrorists. Organized crime impacts the local inhabitants and military operations. It threatens military operations more because it strives to control illicit and legitimate activities among local and regional political, economic, financial, and informational systems to accumulate power. Organized criminals, insurgents, and terrorists use violence to gain control. The structured nature of organized crime often makes link and association methodologies effective tools to identify people, patterns, and locations that can be targeted for a desired effect.

1-18. The "L" in POLICE tells military police planners what the legal system is composed of. It will answer important questions such as the following:

- Is there a law-enforcing mechanism? If so, what is it?
- Is there an adjudicating body?
- Is there a correctional or prison system?

Assessing these components of the legal system may significantly expand the effectiveness of prolonged efforts to ensure safety and security in a complex environment. Tactical and operational transitions are often well planned and rehearsed in military operations and their synchronization is often essential for mission success. Functional transitions, like those that comprise a regional legal system, may occur in a manner that leaves commanders unprepared. The challenge of Operation Restore Hope was increasing the effectiveness of the Haitian policing effort without strengthening the Haitian judicial capabilities. OIF has shown that quickly installing Iraqi judges and penitentiaries is meaningless without a self-reliant police force. Maintaining or developing all major components of a regional legal system is key to success.

1-19. The "I" in POLICE indicates the necessity to conduct investigations in all environments, whether to demonstrate command responsibility, assess critical failures, or capture lessons learned. Military operations in close proximity to civilians, social institutions, and culturally sensitive sites are inherently prone to cause collateral damage or unintended consequences. Belligerents and the inhabitants of complex environments have the capability to leverage information technologies in a manner that makes operations more transparent than in the past. This increase in transparency demands objectivity in the investigative process. Developing a framework through which internal and external investigations, inquiries, and assessments are initiated, managed, tracked, and reported is key to demonstrating responsibility in a transparent environment. Although they require methodical and meticulous work, successful investigations restore confidence and protect lives.

1-20. The "C" in POLICE represents the assessment of crime-conducive conditions that may lead to criminal activity and may become the basis for other threat activity in a complex environment. The crime-conducive conditions represent a relationship between three variables:

- A specific resource (such as food).
- A particular location (such as a food resupply point).
- An enforcement gap (such as a lack of lighting or security persons conducting spot checks).

Crime-conducive conditions must be reduced or prevented because they will ultimately cost commanders combat power and can threaten mission accomplishment at any level of operations. Military police leaders must analyze all phases of tactical operations to identify crime-conducive conditions and their potential impact on operations. Crime-conducive conditions at points of embarkation and debarkation can enable the pilferage or diversion of logistical resources, or they may degrade the fighting spirit of Soldiers if they lead to crimes against persons (such as assault, robbery, or rape in reception and staging areas or base camps). They may threaten lines of communication or maneuver operations. Remove one of the three variables, and the crime-conducive environment no longer exists.

1-21. The "E" in POLICE provides for the analysis of enforcement mechanisms and gaps. Many of the traditional and more obvious enforcement mechanisms present in an OE may be assessed during the IPB process and may be initially listed as friendly or enemy. They could include police and security forces, the border control, the National Guard, or militia organizations. Enforcement mechanisms also include strong and structured religious, ethnic, or family influences as well as organized criminal elements. Deliberately eliminating or degrading enforcement mechanisms identified as threat forces in mission planning can result in the creation of enforcement gaps unless other enforcement mechanisms are present or deliberately

introduced to the environment. When an enforcement gap is created in physical proximity to valuable resources and key terrain or locations, they result in crime-conducive conditions and can destabilize an area. Replacing or replicating an enforcement mechanism can be manpower intensive and vulnerable to cultural sensitivities. Therefore, the process of assessing enforcement mechanisms and enforcement gaps must be carefully considered for every phase of an operation to determine which mechanisms require strengthening vice elimination or transformation.

1-22. POLICE is critical because it provides the tools to military police planners on what areas the G2 and the assistant chief of staff, operations and plans (G3) need to focus on and how to synchronize such collection methods within a fusion cell. Accordingly, the military police planners using POLICE identify key tasks and/or information requirements (IR) for the G2 and G3 to incorporate into subsequent MDMP efforts and taskers for subordinate units.

DEVELOPMENT OF AN EFFECTIVE POLICE INTELLIGENCE OPERATIONS NETWORK

1-23. Synchronization among information collection agencies is accomplished through the development of a PIO network. A PIO network is a network of agencies with the potential to provide police information and CRIMINT and mutual support to other agencies for targeting, collecting, and interdicting purposes or for any other specified intelligence purpose. In addition to CRIMINT, network support can include joint planning, training, and law enforcement operations; consultation for special services such as forensics or investigations; technology support; and resource sharing. In essence, an effective PIO network can provide synergies encompassing CRIMINT activities and law enforcement operations ranging from planning to execution.

1-24. The end state to developing a PIO network is to create a seamless, real-time information network capable of providing actionable intelligence against the full range of threats affecting the OE. ALE personnel must identify and develop partnerships with all available international, military, federal, state, and local agencies in order to develop a successful PIO network. A well-developed and comprehensive PIO network may include the following:

- Law enforcement agencies.
- Criminal, military, and civilian intelligence organizations.
- Security agencies.
- FP agencies.
- Emergency responder services.
- Medical services.
- Other intelligence collectors and analysts, as appropriate.

1-25. *Chapter 7* describes the development of PIO networks in various OEs and the development and management of forums and fusion cells.

1-26. In order for commanders and ALE managers to understand fully how PIO contributes to MI operations, they must first understand ISR and how ISR is synchronized and integrated into the unit's orders production and planning activities. ISR is a critical intelligence task that facilitates the commander's visualization and understanding of the threat and the battlefield. ALE units and organizations contribute information through various detection methods and systematic observations, reconnaissance, and surveillance activities (see *FM 2-0*).

1-27. With staff participation, the S2 synchronizes intelligence support to the ISR effort by focusing intelligence collection, processing, analysis, and products on the critical needs of the commander. The operations officer, in coordination with the S2, tasks and directs the available ISR assets to answer the commander's critical information requirements (CCIR). The ISR task is a continuous process that has the following subtasks:

- Perform intelligence synchronization.
- Perform ISR integration.

- Conduct tactical reconnaissance.
- Conduct surveillance.

For more information on these subtasks, see [Chapter 3](#).

COMMON POLICE INTELLIGENCE OPERATIONS DEFINITIONS

1-28. The following definitions are provided to clarify the ambiguities sometimes associated with the PIO function. These definitions, with exception to PIO and CRIMINT, are from *FM 1-02*. CRIMINT is from *AR 525-13*.

- PIO are a military police function that support, enhance, and contribute to the commander's situational understanding, common operational picture, and FP program.
- Human Intelligence (HUMINT) is a category of intelligence derived from information collected and provided by human sources.
- CRIMINT is the product that results from the collection, analysis, and interpretation of all available information concerning known and potential criminal threats and vulnerabilities of supported organizations.
- Information is unprocessed data of every description which may be used in the production of intelligence. It is the meaning that a human assigns to data by means of the known conventions used in the data's representation. Additionally, information is raw, unanalyzed data that identifies persons, evidence, and events.
- Intelligence, as it relates to foreign sources, is the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. It is also the information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. It is under the auspices of this second definition that ALE personnel perform PIO.
- Law enforcement sensitive (LES) classification is information or intelligence that is obtained for, processed through, or managed by law enforcement organizations. It is essential that this data is restricted to law enforcement channels, unless otherwise directed by competent authority.

APPLICATION OF POLICE INTELLIGENCE OPERATIONS

1-29. PIO bridge the information gap for commanders and leaders. They do so through the police information collection process and the CRIMINT process (described in [Chapters 3](#) and [4](#)) in concert with the MDMP. PIO are a stand-alone military police function that—

- Is conducted throughout the full spectrum of Army operations.
- May be conducted in conjunction with the other military police functions of maneuver and mobility support (MMS), area security (AS), law and order (LO), and internment/resettlement (I/R) operations (see [Figure 1-1](#), page 1-8). The PIO function may be complemented by other forces that collect police information as described in [paragraph 1-5](#).

1-30. PIO are conducted across the full spectrum of operations—peace, conflict, and war. At one end of the spectrum, PIO are integrated with other military police support to continuously refine the commander's battlefield visualization, focus targeting and interdiction, or plan counterthreat measures. At the other end of the spectrum, ALE personnel have experienced an increasingly significant role in countering asymmetric threats often associated with criminal and terrorist activity. [Chapter 5](#) describes PIO in UO, an environment in which commanders face diverse challenges not faced elsewhere and where perhaps PIO are best performed and achieved. [Chapter 6](#) describes the challenges faced by DESs and PMs who conduct the PIO function on installations.

1-31. The collection and study of facts, data, events, or experiences that are related to criminal-oriented behavior and the manner in which the information is processed and applied is an investigative function and core competency of the Military Police Corps and the United States Army Criminal Investigations Command (USACIDC). Critical to this competency is the ability of analysts to identify crime patterns and

trends to assist patrols and investigative units and to aid in the development of the MI community's threat picture and the IPB.

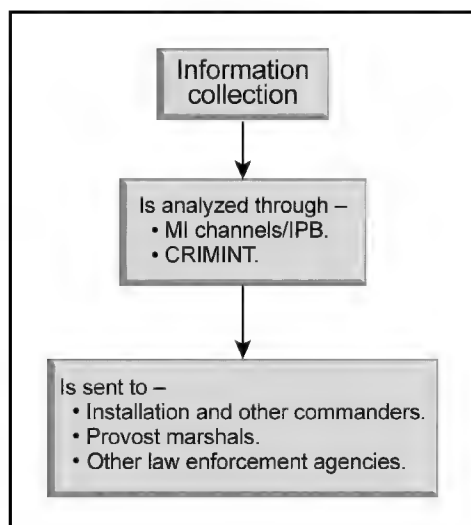


Figure 1-1. Information Sharing Through PIO

1-32. PIO use the CRIMINT process (described in [Chapter 4](#)) to produce actionable police intelligence products used by the Army and the joint community in joint operations in both tactical and nontactical environments. CRIMINT products include criminal threat assessments and strategic and OPLANs to support local HN law enforcement in—

- Combating crime and/or neutralizing criminal threats to military operations based on trend and pattern analysis.
- Disseminating police information and CRIMINT (as applicable) to law enforcement entities. [Appendix B](#) and [Chapter 4](#) discuss these products and procedures, as well as the databases used to capture the police information and CRIMINT to be analyzed. Police intelligence products serve to focus police operations, which in turn contribute to FP and mission success. PIO provide the developed CRIMINT product to the MI community for incorporation and fusion, which contributes to the overall intelligence picture.

1-33. Commanders and military police leaders must ensure the accountability of the PIO function. The execution of the PIO function is most pervasive when engaging in antiterrorism (AT) operations. Providing timely, accurate, and complete information is critical in preventing and deterring terrorist activities and is just as crucial when countering terrorist activities. These same information characteristics apply to organized and entrepreneurial crime, from drug trafficking and the associated crime of money laundering to transnational computer crime (such as Internet fraud or identity theft cartels) and street crime (such as bicycle theft rings). Receiving credible and reliable police information is imperative to developing effective CRIMINT to address criminal and terrorist threats.

ARMY LAW ENFORCEMENT POLICY

1-34. ALE activities are driven by jurisdiction of and compliance with the law. Jurisdiction is distinctly different for the CONUS than outside the continental United States (OCONUS), as are the applicable laws. [Chapter 2](#) of this manual describes the legal instruments that ALE personnel are bound by when performing the duties of collecting, analyzing, and storing information on personnel.

1-35. It is ALE policy to establish common standards, policies, and practices to help expedite CRIMINT sharing. ALE personnel do this while protecting the privacy and rights of citizens as afforded under the laws described in [Chapter 2](#).

Chapter 2

Legal Documents and Considerations

ALE managers, analysts, and police information collectors manage, analyze, and collect police information and CRIMINT under the legal instruments of national and international laws, federal statutes, Department of Defense (DOD) and DA directives and regulations, and the status of forces agreements (SOFAs). ALE personnel are governed by information acquisition regulations, most notably *DODD 5200.27*, and not intelligence regulations. Addressed in this chapter are those documents most prevalent to the PIO collection efforts. A summary of each document (with respect to its relevancy and applicability to the PIO function) and its restrictions and provisions to the ALE's PIO function are described in the following paragraphs.

EXECUTIVE ORDER 12333

2-1. *Executive Order (EO) 12333* provides direction to US intelligence activities and is intended to enhance human and technical collection techniques. While serving that purpose, nothing within the order is to be construed to apply or interfere with any authorized civil or criminal law enforcement responsibility of any department or agency (see [paragraph 2-2](#)).

2-2. This order provides for nonconsensual physical searches in the United States by the Federal Bureau of Investigations (FBI) and other law enforcement activities in specific situations such as "searches by counterintelligence elements of the military services directed against military personnel within the United States or abroad for intelligence purposes, when authorized by a military commander empowered to approve physical searches for law enforcement purposes, based upon a finding of probable cause to believe that such persons are acting as agents of foreign powers."

2-3. The laws governing the sharing of police information and CRIMINT between the law enforcement and intelligence communities are very specific. Generally, intelligence agencies cannot collect, gather, or store information from law enforcement agencies. For exception to this requirement, see *EO 12333, paragraph 2.5*.

2-4. The collection of national foreign intelligence OCONUS is coordinated with the Central Intelligence Agency (CIA) if not otherwise obtainable. Such collection within CONUS is coordinated with the FBI.

2-5. *EO 12333* allows intelligence agencies to—

- Cooperate with appropriate law enforcement agencies for the purpose of protecting the employees, information, property, and facilities of any agency within the intelligence community.
- Participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers or international terrorist or narcotics activities, unless otherwise precluded by law or this order.
- Provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency or, when lives are endangered, to support local law enforcement agencies. The provision of assistance by expert personnel is approved in each case by the general counsel of the providing agency.
- Render any other assistance and cooperation to law enforcement authorities not precluded by applicable law.

2-6. *EO 12333, paragraph 1.6a*, also directs the heads of all executive branch departments and agencies (according to law and relevant procedures approved by the Attorney General under this order) to cooperate with the Director of Central Intelligence in providing information relevant to the national intelligence needs of the United States and to consider requests of the Director of Central Intelligence for appropriate support for intelligence community activities.

DEPARTMENT OF DEFENSE DIRECTIVE 5200.27

2-7. The purpose of *DODD 5200.27* is to establish the general policy, limitations, procedures, and operational guidance pertaining to the collecting, processing, storing, and disseminating of information concerning persons and organizations not affiliated with the DOD. While serving this purpose, nothing in this directive is to be construed to—

- Prohibit the prompt reporting to law enforcement agencies of any information indicating the existence of a threat to life or property or the violation of law, nor to prohibit keeping a record of such a report (*paragraph 6.1*).
- Restrict the direct acquisition of information by overt means (*paragraph 6.2*). Information acquired under this directive will be destroyed within 90 days unless its retention is required by law or unless its retention is specifically authorized under criteria established by the Secretary of Defense (SECDEF) or his designee.

2-8. *DODD 5200.27* provides for the acquisition of information concerning the activities of—

- Individuals and organizations (not affiliated with the DOD) within the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, and US territories and possessions.
- Non-DOD affiliated US citizens anywhere in the world (*paragraphs 2.2, 2.2.1, and 2.2.2*).

2-9. DOD policy prohibits the collecting, reporting, processing, or storing of information on individuals or organizations not affiliated with the DOD, except in those limited circumstances where such information is essential to the accomplishment of DOD missions. Information-gathering activities will be under overall civilian control, with a high level of general supervision and frequent inspections at the field level. Where collection activities are authorized to meet an essential requirement for information, maximum reliance will be placed upon domestic civilian investigative agencies, federal, state, and local. In applying the criteria for the acquisition and retention of information established pursuant to *DODD 5200.27*, due consideration will be given to the need to protect DOD functions and property in the different circumstances existing in geographic areas OCONUS. Relevant factors include—

- The level of disruptive activity against US forces.
- The competence of HN investigative agencies.
- The degree to which US military and HN agencies exchange investigative information.
- The absence of other US investigative capabilities.
- The unique and vulnerable position of US forces abroad.

2-10. *DODD 5200.27, paragraph 4*, authorizes ALE personnel to gather information to accomplish the following defense missions:

- Protection of DOD functions and property. Information may be acquired about activities threatening defense, military, and civilian personnel and defense activities and installations, including vessels, aircraft, communications equipment, and supplies. Only the following types of activities justify acquisition of information under the authority of this paragraph:
 - Subversion of loyalty, discipline, or morale of DOD military or civilian personnel by actively encouraging the violation of law, disobedience of lawful order or regulation, or disruption of military activities.
 - Theft of arms, ammunition, or equipment or the destruction or sabotage of facilities, equipment, or records belonging to DOD units or installations.
 - Acts jeopardizing the security of DOD elements or operations or compromising classified defense information by unauthorized disclosure or by espionage.

- Unauthorized demonstrations on active or reserve DOD installations.
- Direct threats to DOD military or civilian personnel in connection with their official duties or to other persons who have been authorized protection by DOD resources.
- Activities endangering facilities that have classified defense contracts or that have been officially designated as key defense facilities.
- Crimes for which the DOD has responsibility for investigating or prosecuting.
- Personnel security. Investigations may be conducted in relation to the following categories of personnel:
 - Members of the armed forces, including retired personnel, members of the reserve components, and applicants for commission or enlistment.
 - DOD civilian personnel and applicants for such status.
 - Persons having need for access to official information requiring protection in the interest of national defense under the DOD Industrial Security Program or being considered for participation in other authorized DOD programs.
- Operations related to civil disturbance. The Attorney General is the chief civilian officer in charge of coordinating all federal government activities relating to civil disturbances. Upon specific prior authorization of the SECDEF or his designee, information may be acquired that is essential to meet operational requirements flowing from the mission assigned to the DOD to assist civil authorities in dealing with civil disturbances. Such authorization will only be granted when there is a distinct threat of a civil disturbance exceeding the law enforcement capabilities of state and local authorities.

2-11. *DODD 5200.27* identifies those instances in which ALE personnel are prohibited from collecting information on individuals and organizations. The prohibitions are—

- That the acquisition of information on individuals or organizations not affiliated with the DOD will be restricted to that which is essential to the accomplishment of assigned DOD missions under this directive.
- That no information will be acquired about a person or organization solely because of lawful advocacy of measures in opposition to government policy.
- That there will be no physical or electronic surveillance of federal, state, or local officials or of candidates for such offices.
- That there will be no electronic surveillance of any individual or organization, except as authorized by law.
- That there will be no covert or otherwise deceptive surveillance or penetration of civilian organizations unless specifically authorized by the SECDEF or his designee.
- That no DOD personnel will be assigned to attend public or private meetings, demonstrations, or other similar activities for the purpose of acquiring information, the collection of which is authorized by *DODD 5200.27*, without specific prior approval by the SECDEF or his designee. An exception to this policy may be made by the local commander concerned, or higher authority, when, in his judgment, the threat is direct and immediate and time precludes obtaining prior approval. In each such case, a report will be made immediately to the SECDEF or his designee.
- That no computerized data banks will be maintained relating to individuals or organizations not affiliated with DOD unless authorized by the SECDEF or his designee.

ARMY REGULATION 190-45

2-12. CRIMINT and its purpose in determining whether or not an investigation is warranted is discussed in *AR 190-45*. The following fundamentals are covered in *paragraphs 2-5a* through *2-5e* of this AR:

- CRIMINT is gathered to identify individuals or groups of individuals in an effort to anticipate, prevent, or monitor possible criminal activity.
- CRIMINT will be actively exchanged between DOD law enforcement agencies; military police; USACIDC; and local, state, federal, and international law enforcement agencies.

- Written extracts from local police intelligence files provided to an authorized investigative agency must have the following included on the transmittal documents: THIS DOCUMENT IS PROVIDED FOR INFORMATION AND USE. COPIES OF THIS DOCUMENT, ENCLOSURES THERETO, AND INFORMATION THEREFROM, WILL NOT BE FURTHER RELEASED WITHOUT THE PRIOR APPROVAL OF THE INSTALLATION PM.
- Local police intelligence files may be exempt from certain disclosure requirements by *AR 25-55* and the *Freedom of Information Act (FOIA)*.

ARMY REGULATION 195-1

2-13. *AR 195-1* prescribes responsibilities, mission, objectives, and policies pertaining to the USACIDC. It requires commanders to report suspected criminal activity to ALE personnel and requires investigative services to be initiated once notification is made. Criminal incidents in the Army are reported to the military police. Serious criminal incidents, as defined by *AR 195-2*, are reported to CID personnel.

ARMY REGULATION 195-2

2-14. *AR 195-2* requires that the focus of the police information, program be to detect, analyze, and prevent criminal activity from affecting the Army. In part, the purpose of this program is to conduct criminal investigations and crime prevention and CRIMINT activities, to include personnel security, internal security, and criminal and other law enforcement matters, all of which are essential to the effective operations of the Army. This regulation, like *AR 190-45*, requires close coordination between DOD law enforcement agencies; military police; USACIDC; and local, state, federal, and international law enforcement agencies and that police information, and CRIMINT be actively exchanged between them. This interaction between the different agencies allows for the creation of networks, forums, and fusion cells that are described in [Chapter 6](#). These shared, fused systems enhance the ability of ALE personnel to produce timely, accurate, and relevant intelligence that is crucial to the commander's decision-making ability.

ARMY REGULATION 380-13

2-15. *AR 380-13, paragraph 9*, states that no information will be acquired about a person or organization solely because of lawful advocacy of measures in opposition to US government policy or because of activity in support of racial and civil rights interests. It provides other restrictions on the types of information that may be collected as they apply to the intelligence community. *Paragraph 10* allows for prompt reporting to ALE personnel of any information that indicates the existence of a threat to life or property and the violation of a law.

ARMY REGULATION 381-10

2-16. *AR 381-10* is an MI community regulation. However, to clarify what ALE personnel can expect in terms of assistance from MI, the following information is provided. It is important for ALE personnel to understand that the procedures of this regulation do not apply to them. If during an Army intelligence component investigation, evidence surfaces that provides reasonable belief that a crime has been committed, details of the investigation will be relinquished to the USACIDC or the appropriate military police investigating agency, according to *ARs 195-2, 190-45, and 381-20*.

2-17. Agencies from within the MI community are authorized to—

- Cooperate with law enforcement agencies for the purpose of protecting the employees, information, property, and facilities of any agency within the intelligence community.
- Participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign equipment or technical knowledge or to provide assistance of expert personnel for use by any department or agency or, when lives are endangered, to support local law enforcement agencies unless otherwise precluded by law or *AR 381-10*. The provision of

assistance by expert personnel will be approved in each case by the general counsel of the providing agency.

- Render any other assistance and cooperation to law enforcement authorities not precluded by applicable law.

2-18. ALE personnel can expect cooperation (consistent with *DODD 5525.5*) from the MI community for the purpose of—

- Investigating or preventing clandestine intelligence activities by foreign powers, international narcotics activities, or international terrorist activities.
- Protecting DOD employees, information, property, and facilities.
- Preventing, detecting, or investigating other violations of law.

2-19. A significant item that *AR 381-10* highlights is the definition of "collect." Within the text of this AR, its use is different from that of everyday common usage such as to assemble or to gather. Within *AR 381-10*, collect includes the intent to use or retain the information received and also includes using information received from cooperating sources in the collection effort. The intent of this definition, although not stated within this regulation, is also the intent of information collection efforts by ALE personnel.

ARMY REGULATION 525-13

2-20. *AR 525-13, paragraph 2-17*, states that the USACIDC will—

- Collect, analyze, and disseminate to affected commands CRIMINT pertaining to threat activities, within the provisions of applicable statutes and regulations.
- Maintain a capability to analyze and disseminate collected, time-sensitive information concerning the criminal threat against Army interests.
- Provide appropriate threat-related CRIMINT to Headquarters, Department of the Army (HQDA) (Antiterrorism Operations Intelligence Cell [ATOIC]), the Intelligence and Security Command (INSCOM), and Army Counterintelligence Center (ACIC).
- Investigate threat incidents of Army interest and to monitor such investigations when conducted by civilian, HN, military, or other police agencies. Provide applicable results of terrorist-related investigations to HQDA (ATOIC), ACIC, and the Center for Army Lessons Learned (CALL).
- Provide trained hostage negotiators to support Army AT operations worldwide.
- Plan and coordinate the protection of high-risk personnel for DOD, DA, and foreign officials as directed by HQDA.
- Serve as the Army's primary liaison representative to federal, state, and local agencies and HN agencies to exchange CRIMINT.
- Ensure that those personal security vulnerability assessments (PSVAs) conducted in support of high-risk person (HRP) security programs consider potential attacks by terrorists.
- Establish procedures to ensure appropriate liaison at all levels between USACIDC, INSCOM, and PM/security officer (SO) elements operating in support of the AT program.
- Immediately notify the affected installation PM/SO and HQDA (in accordance with [Appendix C](#)) upon receipt of time-sensitive threat information.
- Conduct domestic CRIMINT collection efforts and disseminate information on domestic criminal threats against the Army.
- Implement criminal investigative measures, crime prevention efforts, and criminal investigations to protect the Army's command and control (C2) systems and to respond to criminal attacks and intrusions.
- Consolidate relevant C2 protect AT inputs and provide to the Office of the Deputy Chief of Staff for Operations and Plans (ODCSOPS) in support of information operations (IO) policy.
- Assess specific and general Army C2 vulnerabilities open to criminal activity, and recommend corrective actions to eliminate or mitigate them in coordination with the Land Information Warfare Activity (LIWA).

- Perform criminal threat and vulnerability assessments for Army personnel, installations, systems, operations, and other interests as directed by HQDA and/or based on Army commanders' operational requirements.
- Provide technical personnel support to ODCSOPS-designated assessment teams, as required.
- Investigate all incidents of suspected terrorism as criminal acts, to include safeguarding of evidence, collection testimony, preparation of investigative reports, and presentation to appropriate judicial officials. Investigations will be conducted jointly with federal, state, local, and foreign law enforcement agencies, as appropriate.
- React to and assess Army computer security incidents (that is, unauthorized root use or access, denial of service, and so forth) to determine if criminal acts were perpetrated, and investigate those related crimes as appropriate in coordination with the Army Computer Emergency Response Team (ACERT) and INSCOM.
- Conduct computer crime and information assurance vulnerability assessment in conjunction with director of information systems for command, control, communications, and computers (DISC4) and the LIWA, examining for early I&W of terrorist and/or criminal activities involving Army or DOD information systems.
- Provide liaison to the Joint Task Force-Computer Network Defense for law enforcement and criminal investigative matters involving attacks on Army information systems.
- Provide domestic terrorism analysis and threat assessments to the ATOIC in support of Army requirements and the AT program.
- Ensure a sufficient USACIDC CRIMINT capability to monitor and report on the activities, intentions, and capabilities of domestic threat groups according to applicable regulations and directives.

2-21. *AR 525-13, paragraph 4-3*, directs that commanders at installation level and above will have a fully integrated foreign, domestic, and CRIMINT AT intelligence program focused and based on PIR that provide the appropriate threat information to protect personnel, family members, facilities, material, and information in all locations and situations. Commanders will also ensure that the appropriate intelligence and law enforcement organizations within their command collect and analyze criminal threat information. *Paragraph 4-3* also mandates that collection operations be conducted consistent with the requirements of *ARs 381-10, 381-12, 380-13, DODD 5200.27*, and other regulations and directives and that the command have appropriate connectivity to receive threat-related information from all available sources, such as the FBI and Intelink-S.

2-22. *Paragraph 4-3* also states the following:

- Threat information prepared by the intelligence community, USACIDC, and the Provost Marshal Office (PMO) will be used when conducting threat assessments as well as technical information from information management.
- Threat assessments will serve as a basis and justification for AT plans, enhancements, program/budget requests, and the establishment of force protection conditions (FPCONs).
- Threat assessments will be part of a leader's reconnaissance in conjunction with deployments and follow-on threat and vulnerability assessments will be conducted as determined by the commander.
- Consolidated MI and CRIMINT data identified in threat assessments (on US persons) cannot be filed, stored, or maintained as an intelligence product, according to *AR 381-10*. These assessments must be filed, stored, and maintained within operational channels.

CRIMINAL INVESTIGATIONS DIVISION REGULATION 195-1

2-23. *CID Regulation 195-1* defines CRIMINT as "information obtained, compiled, and indexed for use during the conduct of investigations, and to anticipate, analyze, prevent, or monitor possible or potential criminal activity directed at or affecting the US Army, or Army personnel."

2-24. Additional ARs that may provide assistance to ALE personnel in the conduct of PIO (specifically information and reporting) are—

- *AR 190-6.*
- *AR 190-27.*
- *AR 190-40.*

DEPARTMENT OF DEFENSE DIRECTIVE 2000.12 AND DEPARTMENT OF DEFENSE INSTRUCTION 2000.16

2-25. *DODD 2000.12* and *Department of Defense Instruction (DODI) 2000.16* provide direction to ALE personnel on their role in threat assessment. *DODD 2000.12, paragraph 5.16.10*, states that—

- An assessment of the capability of the military departments, the combatant commands, and the defense intelligence and security organizations to collect, receive, evaluate, analyze, and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack will be conducted.
- An assessment of the capability to fuse suspicious activity reports from military security, law enforcement, and counterintelligence organizations with national-level ISR collection activities will also be conducted.

2-26. *Paragraph 5.17.15* directs commanders to ensure that a capability exists to collect, receive, evaluate, analyze, and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack and develop the capability to fuse suspicious activity reports from military security, law enforcement, and counterintelligence organizations with national-level ISR collection activities.

2-27. *DODI 2000.16, paragraph E3.1.1.8*, directs commanders to task the appropriate organizations under their command to gather, analyze, and disseminate terrorism threat information, as appropriate. *Paragraph E3.1.1.8.1* states that services should continually ensure that forces are trained to maximize the use of information derived from law enforcement liaison and intelligence and counterintelligence processes and procedures. This includes intelligence procedures for handling priority intelligence requests for in-transit units and the implementation of procedures to conduct IPB and mission analysis.

2-28. *Paragraphs E3.1.1.8.2 and E3.1.1.8.3* highlight the fact that identifying potential terrorism threats is the first step in developing an effective AT program and that commanders who understand this threat can assess their ability to prevent, survive, and prepare to respond to an attack. In order to make these assessments, the analysis of all available information must be made. In addition to the information collection tasking, commanders should encourage personnel under their command to report information on individuals, events, or situations that could pose a threat to the security of DOD personnel, families, facilities, and resources.

USA PATRIOT ACT

2-29. The *Patriot Act* allows investigators to use the tools that were already available to investigate organized crime and drug trafficking. It allows—

- Law enforcement to use surveillance against crimes of terror.
- Federal agents to follow sophisticated terrorists trained to avoid detection.
- Law enforcement to conduct investigations without tipping off terrorists.
- Federal agents to ask a court for an order to obtain business records in national security terrorism cases.

2-30. The *Patriot Act* has had the greatest impact on—

- Enhancing the federal government's capacity to share intelligence.
- Strengthening the criminal laws against terrorism.
- Removing obstacles to investigating terrorism.
- Updating the law to reflect new technology.

2-31. The realization of the *Patriot Act* for ALE personnel is that under the—

- Old law, grand jury information could only be disclosed by court order under restricting rules and there was no provision for sharing national security information discovered (*Section 203*).
- New law, the disclosure of foreign intelligence, counterintelligence, or foreign intelligence information to any federal law enforcement, intelligence, protective, immigration, national defense, or national security official is allowed in order to assist in official duties, as the court may direct.
- Old law, wiretap information was allowed to be disclosed (full-content voice and electronic communications) to assist in criminal investigations.
- New law, investigative or law enforcement officers are allowed to disclose foreign intelligence information without a court order to any other federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist in official duties. The new law also allows disclosure of foreign intelligence information from criminal investigations to any federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist in official duties.
- Old law, enforcement officers could use search warrants for voice recording on an answering machine inside a criminal's home (easier), but required a wiretap order for voice communications with a third party provider (*Section 209*).
- New law, stored voice (wire) communications are acquired under *Title 18 United States Code (USC) 2703 (18 USC 2703)* (including search warrants).
- Old law, subpoenas were limited to the customer's name, address, length of service, and means of payment (*Section 210*).
- New law, the records that are available by subpoena are expanded. Subpoenas can now obtain the means and source of payment, credit card or bank account numbers, records of session times and durations, and any temporarily assigned network address.
- Old law, law enforcement had restricted to most cable company records. The customer was required to have prior notice and was entitled to the right to a hearing. Disclosure would only result if clear and convincing evidence of reasonable suspicion of a crime was present (*Section 211*). (Cable companies also provide Internet and telephone services.)
- New law, the Electronic Communications Privacy Act and trap and trace rules that govern cable company records for telephone and Internet services are much clearer. The act keeps the same procedures for ordinary cable television programming. The importance of this new provision is that it brings cable communications services into line with other communication mediums.

STATUS OF FORCES AGREEMENTS AND INTERNATIONAL LAW

2-32. The requirements of these legally binding instruments will vary from one location to the next. Since 1975, a provision known as *Section 660 of Title 22 USC 2420 (22 USC 2420)* has restricted the use of foreign assistance funds for foreign law enforcement, including training. These restrictions were designed to distance the US from controversy over police violations of human rights and do not apply in countries with longstanding democratic traditions. A variety of exceptions to *Section 660* have been exacted over the years, but it still restricts DOD's role in foreign law enforcement training. Commanders must consult with their local staff judge advocate (SJA) regarding these instruments to determine their restrictions on PIO collection efforts in a given area.

Chapter 3

Police Intelligence Operations as Emerging Doctrine

Traditionally, ALE personnel performed many of today's police intelligence activities at local levels using informal systems. They focused primarily on collecting, reporting, and processing and placed less emphasis on analysis and production, dissemination and integration, and staff responsibilities. Given current national trends that emphasize intelligence-led policing, PIO doctrine can be expected to expand for the foreseeable future. PIO can work to reduce threats against Army installations; provide threat intelligence for in-transit security; and focus the development and implementation of threat countermeasures to safeguard Army personnel, materials, and information. Effective PIO provide commanders with situational understanding, contribute to achieving the desired results of EBO, and address information gaps to ensure that threat assessments are both valid and reliable.

EFFECTIVE POLICE INTELLIGENCE OPERATIONS DEVELOPMENT

3-1. The success of the PIO function depends on the following processes:

- Command staff process.
- Police information collection process.
- CRIMINT process (see [Chapter 4](#)).

COMMAND STAFF PROCESS

3-2. The command staff is comprised of division, brigade, and battalion commanders and/or PM staff, (to include the CRIMINT analyst when assigned). The personnel responsible for the command staff process direct the PIO function and conduct the criminal analysis. They request, receive, and update the IPB. Once they have made an assessment of the IPB, they use the MDMP and determine the COA for the criminal threat and the CCIR for police information collection efforts. CCIR are those elements of information required by commanders that directly affect decision making and dictate the successful execution of military operations. The commander decides what information is critical based on his experience; the mission; the higher commander's intent; and the command staff's input, such as the initial IPB, police and other information or intelligence, and recommendations (see *FM 3-0*). When in doubt, commanders should consult with the SJA to ensure that the CCIR are aligned with *DODD 5200.27*, the information acquisition directive for ALE units. [Figure 3-1](#), page 3-2, depicts the actions of the command staff process and the continuous nature of those actions.

3-3. The command staff develops the police information collection plan using the requirements of the ISR plan. The police information collection plan will be sent to ALE units to initiate collection efforts and to criminal analysts who may use it during CRIMINT development. Military police conduct reconnaissance and surveillance (R&S) in support of PIO and the ISR plan collection efforts. Through various detection methods and systematic observation, military police conduct R&S (described later in this chapter) to obtain required information to support the CCIR. The results of ALE collection efforts will be fed into the CRIMINT process and the intelligence process. Products resulting from the CRIMINT process will be fed

into the intelligence process. The results of the police information collection effort and the products of the CRIMINT process will ultimately contribute to situational understanding. Some of the considerations a staff must make for a police information collection plan are provided. These considerations may be modified to meet the needs of the mission.

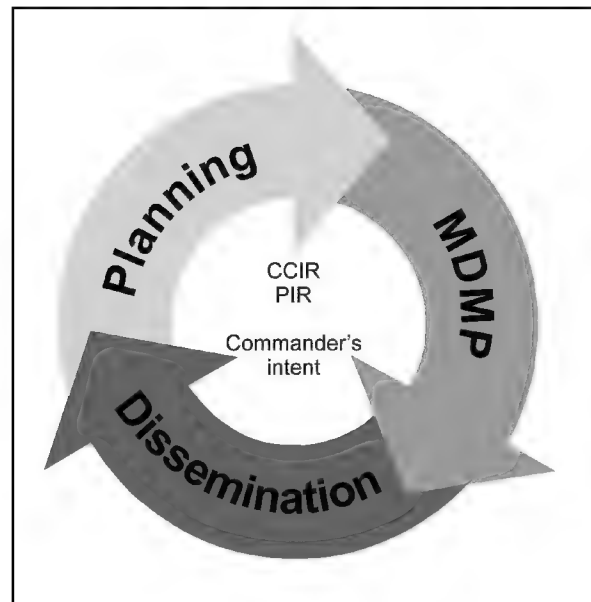


Figure 3-1. Command Staff Process

3-4. *Figure 3-2* depicts how police information and CRIMINT products augment the intelligence process (see *FM 2-0*) in support of the operations process (see *FM 3-0*).

PLANNING AND DIRECTING

3-5. The first responsibility of the staff is to plan and direct PIO. The S2 or operations staff officer (S3) is responsible for the day-to-day operations of PIO or critical activities such as planning and directing or analysis and production (see *Appendix C*). The PIO manager, whether a PM, brigade or battalion S2/S3, company operation officer, or fusion cell manager, provides oversight by—

- Understanding the overall PIO function and its processes.
- Disseminating and nominating the CCIR.
- Reviewing intelligence flow to synchronize tasks and resources.
- Planning and directing PIO and preparing the police information collection plan.
- Establishing guidelines to minimize the discretion of information collectors.
- Establishing procedures to debrief collectors to gather detailed information not recorded in their reports.

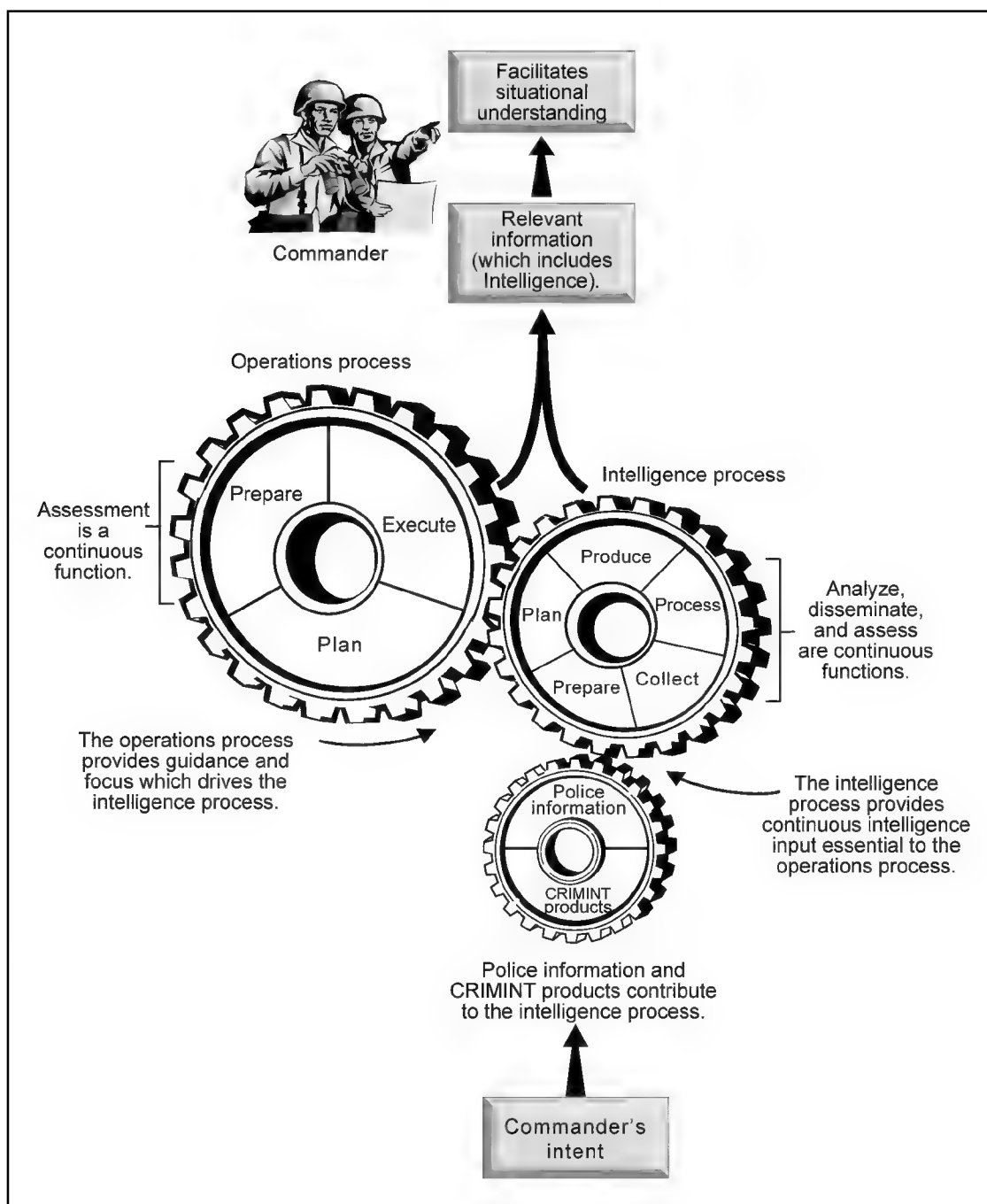


Figure 3-2. Police Information and CRIMINT Products Input into the Intelligence Process

3-6. The commander's intent, planning guidance, and CCIR drive the planning of CRIMINT operations. Planning and directing identifies the CCIR, sets priorities for collection or interdiction, and provides guidance for the management of collection or interdiction assets. Planners should consider the following factors:

- What activities or indicators will confirm the threat?
- Where are probable locations positioned? Locations include named areas of interest (NAIs) and points of vulnerability or target value, such as mission-essential vulnerability areas (MEVAs) and high-risk targets (HRTs).
- When will the threat event occur? This may be predicted by I&W, such as the following in the case of a demonstration:
 - Orientation. Crowd dynamics change from people milling around and talking among themselves in isolated groups to a more collective focus concentrated on a single objective, such as a government figure or specific agitators.
 - Massing. The crowd begins to mass or tighten into a large contiguous body from a loose formation to a static congregation located in a more concentrated area. Unchecked massing can provide anonymity and a collective feeling of invulnerability. This change in group dynamics could provide ideal conditions for a civil disturbance.
 - Outside influence. The presence of people from outside of the community may indicate more sophisticated planning and resourcing than would otherwise be expected from local community members. Although instigators, outside people may feel insulated from responsibility for local actions and, therefore, provide a dangerous catalyst for a violent civil disturbance.
 - Surveillance. Individuals who are conducting surveillance or countersurveillance for unknown reasons.
- What justifies the CRIMINT requirement? This justification prioritizes collection and interdiction efforts.

3-7. Collection involves the gathering of relevant data and raw information or intelligence products to produce actionable intelligence. To be effective, collection efforts are generated and driven by the MDMP; they must be planned, focused, and directed based on the commander's critical information and CRIMINT requirements. This implies developing a collection strategy, tasking specific collectors, and supervising the collection effort.

3-8. The collection of police information and CRIMINT is enabled by, and subject to, the laws, regulations, and policies described in *Chapter 2*. These documents ensure the proper conduct of CRIMINT operations. They include the following:

- The USC.
- An EO.
- National Security Council Intelligence Directives.
- ARs.
- SOFAs.
- Rules of engagement (ROE).
- Other international laws and directives.

DEVELOPING A POLICE INFORMATION COLLECTION STRATEGY

3-9. After a thorough evaluation of the availability, capability, and disposition of the potential collecting resources, ALE leaders select which asset is suitable to perform the collection mission. A good collection strategy answers the following:

- Are organic ALE personnel the best collectors for this mission?
- Are special-skilled personnel required? If so, who?

- Is specialized equipment needed? If so, what kind?
- Should the collection effort be conducted while personnel are performing one of the other military police functions (MMS, AS, or L&O)?

3-10. Part of the collection strategy includes coordinating with the S2/G2, SJA, CID, and other agencies before initiating the collection mission. This coordination will help eliminate duplication of effort, interference with an ongoing effort, or violation of legal limitations.

3-11. Once priorities have been set and a collection strategy developed, a police information collection plan is prepared based on the intelligence requirements, commander's guidance, available collection assets, and other factors, including time and self-protection.

DEVELOPING THE POLICE INFORMATION COLLECTION PLAN

3-12. Planning, managing, and coordinating police information collection operations are continuous activities necessary to obtain police information and produce CRIMINT essential to decision making. Once the commander receives the police information collecting and reporting mission from higher headquarters, he initiates the MDMP identified in [Appendix A](#).

3-13. CRIMINT analysts assist the commander and his staff in identifying the gaps in IR that will help complete the threat picture. This process is described in [Chapter 4](#).

3-14. The commander selects and prepares collection assets based on their capabilities and limitations. ALE personnel are trained collectors, highly adaptable to any collection plan. They operate in direct contact with the local population, allowing them to spot, assess, and interact with potential sources of information. ALE personnel can effectively collect data—

- As an independent mission.
- While conducting any of the other military police functions.
- While providing support to FP.

3-15. In tactical environments and UO, as enemy forces are bypassed or as other threats emerge, ALE personnel may be tasked as the primary collectors of information on enemy forces operating along extended lines of communications and on main supply routes (MSRs). As threat levels are reduced from a military threat to a more asymmetric threat (such as criminal activity associated with stability operations), ALE personnel provide the main effort for police information collection. On military installations, ALE personnel provide the lead for targeting, collecting, and interdicting against a broad range of threat activities including terrorism, organized crime, contraband trafficking, and illegal activities associated with civil disturbance.

3-16. Missions that may result in police information collection opportunities include—

- Patrols (mounted and dismounted).
- Cordon and search operations.
- Checkpoints and roadblocks.
- Traffic control points (TCPs).
- R&S.
- Law enforcement raids.
- Emergency responder services.
- Criminal investigations.
- Field interviews.
- Dislocated civilian operations.
- Access control operations.
- Physical security inspections.

3-17. The staff develops the collection plan, which is used in the police information collection process. This process is described in *paragraphs 3-23* and *3-24*, page 3-8, and depicted in *Figure 3-3*. The staff provides detailed information and instructions to each subordinate unit that may include—

- The method the unit will use to get to its assigned area (routes, passage points, boundaries, and so forth).
- The collection objectives.
- The specific collection tasks (PIR with indicators) and where to look (NAI).
- The start and termination times for collection or surveillance operations and the time the information is needed.
- The report procedures (for example, to whom and on what frequency net to report).
- The location and activity of other units operating in the AO.
- The identification and coordination for linguists or special skills personnel (such as HN police, psychological operations [PSYOP], civil affairs [CA], and MI).

3-18. The most common collection efforts are accomplished through R&S (which is discussed in *Chapter 1*). When performing an R&S mission, it is important to orientate the collection asset on the NAI in a timely manner, report all information rapidly and accurately, complete the mission within the specified time, and answer the IR. The ALE version of the R&S plan most typically used is the patrol distribution plan (PDP). This plan is described later under the CRIMINT process (see *Chapter 4*).

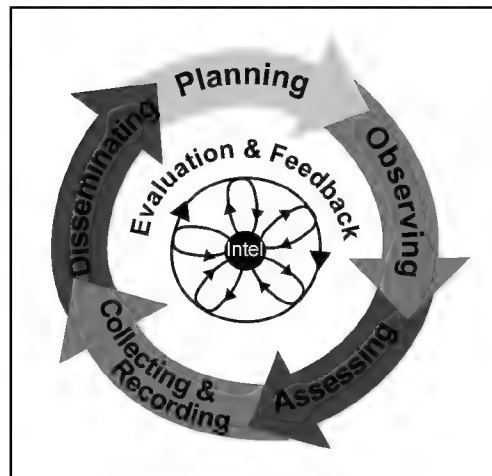


Figure 3-3. Police Information Collection Process

TASKING COLLECTORS

3-19. The missions that will be tasked to respective collectors must be determined. Information collectors can be tasked with more than one mission at a time. However, it is imperative that their tasks be prioritized based on mission requirements and time available. The appropriate tasking or request chain must be used to request linguists, MI, CA, and PSYOP personnel or other special skill personnel such as USACIDC special agents.

3-20. In order for collectors to provide effective information, they must—

- Understand the overall PIO function and its processes as it relates to collection.
- Understand and execute the collection plan.

- Understand the priority for collection based on the CCIR that were developed according to information, acquisition laws and regulations, and the commander's guidance.
- Alert leaders to immediate actionable information.
- Network with other agencies for police information collection.
- Familiarize themselves with the questioning tools in [Appendixes D](#) and [E](#) and understand how they serve as a source of information collection.

ASSESSING AND SUPERVISING THE COLLECTION PLAN

3-21. During PIO execution, the staff continues assessing the effectiveness of the collection effort and the results and products derived from it. The critical aspects of assessments at this point are to determine if the PIR have been answered, which collection efforts are most effective, and which efforts should be adjusted or eliminated. The continual assessment of PIO, collection assets, available information and intelligence, and the dynamics of the OE are critical to—

- Ensure that the CCIR are answered.
- Ensure that CRIMINT requirements are met.
- Redirect collection assets to support changing requirements.
- Ensure that all relevant information is analyzed and disseminated.

CONDUCTING A DEBRIEFING OR AN AFTER-ACTION REVIEW

3-22. The battalion staff is responsible for conducting a debriefing or an after-action review (AAR) at the completion of a mission. Leaders should not consider the mission complete and the personnel released until the reporting and debriefing actions have occurred. All Soldiers, to include leaders returning from meetings, are a potential source of information and must be debriefed by a designated person, such as the S2 or S3 to ensure that collected information gets into the intelligence system. See [Appendix F](#) for debriefing and AAR considerations.

POLICE INFORMATION COLLECTION PROCESS

3-23. The success of the police information collection process depends on its skillful management and execution. When the collection unit being tasked, such as a combat support military police company, receives the collection plan, the company commander and his operations section have the following responsibilities:

- Review the higher headquarters police information collection plan (which will be identified within the MDMP products) and identify the collection requirements.
- Implement the plan by—
 - Tasking subordinate collection elements.
 - Specifying the parameters in which to make discretionary decisions regarding police information collection efforts.
- Update the collection plan as necessary.
- Perform combined police IO by—
 - Maintaining liaison with HN authorities, military and civilian police agencies, and other organizations.
 - Collecting police information.
 - Assessing police information.
 - Exchanging police information with HN authorities, military and civilian police agencies, and other organizations.

- Perform police information collection efforts by—
 - Maintaining liaison with HN authorities, military and civilian police agencies, and other organizations.
 - Collecting police information.
 - Exchanging police information with HN authorities, military and civilian police agencies, and other organizations.
- Perform operational intelligence collection efforts by—
 - Maintaining liaison with HN authorities, military and civilian police agencies, and other organizations.
 - Collecting information according to the ISR collection plan.
- Report police information and CRIMINT through appropriate channels (such as the S2/G2, S3/G3, S5/G5, and military police and intelligence channels) by—
 - Forwarding operational information and CRIMINT to the S2/G2 by means of formal and informal reports and a debriefing or an AAR.
 - Forwarding police information and CRIMINT to the CRIMINT analyst.

3-24. These responsibilities compose the first phase (planning) of the police information collection process. The subordinate collection elements of the company execute all phases of the police information collection process. *Appendixes E* and *F* may further assist in the collection efforts.

- Planning. The collector implements the higher headquarters plan.
- Observing. The collector observes the area and/or activity.
- Assessing. The collector determines the value and application of what he has observed to the CCIR and the police information collection requirements.
- Collecting and recording. The collector documents his observations through reports, sketches, photographs, and other means.
- Disseminating. The collector sends his recorded observations and assessments through established channels. The report phase involves many considerations and, as such, will be discussed at length.
- Evaluation and feedback. The collector uses evaluation and feedback to determine whether or not the requested information was provided and whether or not it supports the PIR and CCIR.

REPORTING PROCEDURES

3-25. Timely and accurate reporting of information is a critical activity of police information collection that is performed by all police agencies. However, the most critical information is worthless if it is not reported in a timely manner. For ALE personnel, the natural flow of police information is through established systems and protocols, such as communications links, reports, and database sequencing. During the collection efforts of directed police information and CRIMINT, collectors must be provided with specific reporting guidelines. ALE assets must know when, how often, and what format to use when reporting police information and CRIMINT. Police information and collection reporting procedures must be described in unit standing operating procedures (SOPs) and operation orders (OPORDs). Information of immediate interest to the commander should be transmitted to the S2 or senior criminal analyst as soon as the situation allows.

3-26. Reports can be transmitted by verbal means or in writing by using Internet protocol services. Reports are also recorded and submitted as hard copy. Commanders and staff must not delay reports for the sole purpose of editing and ensuring the correct format. There are numerous ALE reports used for a variety of activities such as military police reports, investigation reports, situation reports (SITREPs), debriefing reports, and spot reports. The Army's recognized means of reporting information is through a size, activity, location, unit, time, and equipment (SALUTE) report (see *Figure 3-4*).

3-27. The most common report format used by a patrol to report information gathered is the SALUTE report. Before reporting the elements of this report, the patrol identifies itself and its location.

3-28. The SALUTE report format requires brief entries which require the collector to break information into basic elements: who, what, where, when, why, and how. This allows for efficient reporting via an electronic or a hard-copy medium. It allows the analyst to scan multiple reports quickly to find specific information.

Line One - (S)ize/Who: Expressed as a quantity and an echelon or size (for example, 1 x tank). If multiple units are involved in the activity being reported, there can be multiple entries (for example, 1 x tank; 10 x foot Soldiers). Nonstandard units are reported as such (for example, bomb-making class; support staff, 150 chemical rounds).

Line Two - (A)ctivity/What: This line relates to the PIR being reported on and should be a concise bullet statement.

Line Three - (L)ocation/Where: Generally a grid coordinate including the 100,000-meter grid zone designator. This line can also be an address, if appropriate, but still should include an 8-digit grid coordinate. If the activity being reported involves movement (for example, advance, withdrawal), the location entry will include "From" and "To" entries. The route used will be reported under "Equipment/How."

Line Four - (U)nit/Who: This line identifies who is performing the activity described in the "Activity/What" line. Include the complete designation of a military unit, the identification of a civilian or insurgent group, or the full name of an individual, as appropriate.

Line Five - (T)ime/When: This line is when the unit will begin an activity. Ongoing events are reported as such.

Line Six - (E)quipment/How: The information reported in this line clarifies, completes, and/or expands upon information reported in any of the previous entries. It includes information concerning equipment involved, tactics used, and any essential elements of information (EEI) not reported in the previous paragraph.

Note: This sample SALUTE report is for guidance and not meant as a strict requirement. SALUTE reports of combat activity may only contain a word or two in each line, whereas intelligence reports tend to include more detail.

Figure 3-4. SALUTE Report

REPORTING ENTRY POINTS

3-29. While the means for transmitting reports can vary, it is important that reporting is standardized and that reporting through data entry points is fully understood by all collectors to ensure report timeliness. Entry points may include the following:

- Military police battalion operations center.
- Military police desk sergeant (military police station).
- Installation emergency operations center (EOC).
- Tactical operations center.
- Joint law enforcement operation center.
- CID resident agency.

3-30. Units may require classified and unclassified network connections for their equipment. If elements of the unit will be working outside the range of the unit's communications systems, then it is necessary to coordinate for global or extended range communications. In order to retain and account for reported police information, reporting entry points maintain databases, which are discussed in [Chapter 4](#).

RECONNAISSANCE AND SURVEILLANCE

3-31. Military police are a critical part of the commander's on-the-ground information and intelligence gathering assets. Military police teams are mobile over large geographical areas and routinely travel the battlefield and road networks as part of their security mission. They routinely move off-road for area reconnaissance and key terrain observation.

CONDUCT RECONNAISSANCE

3-32. Reconnaissance is a mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy and the meteorological, hydrographic, or geographic characteristics of an AO.

3-33. MI personnel and organizations can conduct reconnaissance by obtaining information derived from signals, imagery, measurement of signatures, technical characteristics, human interaction, and other detection methods.

3-34. The military police conduct area, zone, and route reconnaissance while performing military police functions such as MMS, AS, L&O, and PIO. While conducting various reconnaissance missions, military police often operate in close contact with the local population, allowing for human interaction to spot, assess, and observe potential threat activity (see *FM 7-15*).

3-35. When performing reconnaissance, it is important to—

- Orientate the reconnaissance asset on the NAI and/or reconnaissance objective in a timely manner.
- Report all information rapidly and accurately.
- Complete the reconnaissance mission not later than the time specified in the order.
- Answer the requirement that prompted the reconnaissance task.

CONDUCT SURVEILLANCE

3-36. Conducting surveillance means systematically observing the airspace, surface areas, subsurface areas, places, persons, or things in the AO by visual, aural, electronic, photographic, or other means. Other means may include, but are not limited to, space-based systems and special chemical, biological, radiological, and nuclear (CBRN); artillery; engineer; and air defense equipment (see *FMs 7-15* and *3-90*).

3-37. The military police often conduct visual, electronic, and photographic surveillance activities while conducting L&O and PIO functions. The military police maintain continuous surveillance of NAIs or enemy reconnaissance avenues of approach into a particular sector. This is accomplished by setting up a series of observation posts (OPs). Military police may conduct active mounted patrols to extend their observation limits or to cover dead space and the area between OPs (see *FM 3-19.4*).

3-38. Surveillance activities include—

- Orientating the surveillance asset on the NAI and/or the surveillance objective in a timely manner.
- Reporting all information rapidly and accurately.
- Completing the surveillance mission not later than the time specified in the order.
- Answering the requirement that prompted the surveillance task.

Chapter 4

The Criminal Intelligence Process in Support of Police Intelligence Operations

CID Regulation 195-1 describes the duties of the persons responsible for the CRIMINT program beginning with the office of the Deputy Chief of Staff for Operations, Headquarters, USACIDC down through the CRIMINT manager who acts as the focal point for all CRIMINT within his area of responsibility (AOR), to the special agent in charge (SAC). The CID has the primary responsibility for operating the CRIMINT program, which is designed to obtain, record, analyze, and disseminate information concerning criminal activities directed against, involving, or affecting US Army operations, material, or personnel. CRIMINT is also used to develop, analyze, and report on the methods of operations used in criminal activities and assess the vulnerability of Army operations to crimes. The focus of the CRIMINT program is the detection, collection, analysis, dissemination, and prevention of criminal activity affecting the Army. It is from these directives and responsibilities that the CRIMINT process has evolved.

CRIMINAL INTELLIGENCE PROCESS

4-1. The CRIMINT process, conducted by the CRIMINT analyst, is an integral aspect of PIO. It is used to develop the criminal threat picture, which contributes to the overall threat picture in the IPB. Its purpose is to convert police information and raw data into usable and/or actionable CRIMINT. On military installations, the military police CRIMINT analyst, in coordination with the CID's senior intelligence manager, is generally the primary police information and CRIMINT manager. Likewise, when in support of a military police combat support unit where police information, is being collected, analyzed, and stored, the analyst assumes the role of CRIMINT manager for the commander.

4-2. In military police combat support units where a CRIMINT analyst is assigned, the analyst supports the battalion S2 in the intelligence efforts. The analyst's responsibilities include identifying individuals or groups of individuals in an effort to anticipate, prevent, or monitor possible criminal activity. In concert with the S2, the analyst may be required to manage PIO. These activities include—

- Prioritizing incoming data according to collection and production requirements.
- Organizing police intelligence by category, such as crime or threat, and by particular product or user.
- Entering information into databases.
- Collating actionable police intelligence into interim products.

Note: Products are rarely considered final because analysts rarely have all the information they want to develop CRIMINT since the information evolves as gaps are identified.

4-3. The discussion of this process is not to be misconstrued as or confused with the actions of the battalion (or brigade) staff. Many actions of a CRIMINT manager parallel those taken by the staff. It is important to understand that these procedures are used by the CRIMINT manager to effectively manage and execute the CRIMINT process and to provide the most accurate and timely criminal threat picture to

the S2/S3 or PM. It is critical that the analyst understand the CCIR and the commander's intent when planning the collection efforts of police information, in the CRIMINT process. This process contributes to the efforts of the battalion staff in the information collection process.

4-4. The CRIMINT process consists of the following six phases, as depicted in *Figure 4-1*:

- Planning and directing.
- Collecting and recording.
- Processing.
- Analyzing and producing.
- Disseminating and integrating.
- Evaluation and feedback.

The six phases are discussed in the following paragraphs, such as what occurs within each phase, how each phase of the process connects to the other phases, and how the process as a whole connects to the command process and the police information collection process.

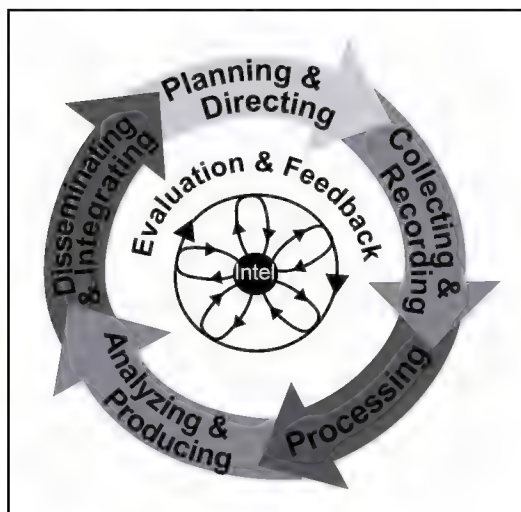


Figure 4-1. CRIMINT Process

PLANNING AND DIRECTING

4-5. This phase of the CRIMINT process outlines the overall effort of CRIMINT development, from identifying the need for information to delivering the CRIMINT product to the commander, staff, or end user. The end user includes everyone with an authenticated need to know, such as the staff directing the PIO function, the installation or combatant commander, ALE operators at all levels, and the MI community. As in any military operation, planning is the first step in the CRIMINT process.

4-6. In this phase, the CRIMINT analyst identifies the commander's intent, reviews the CCIR, sets priorities, and provides guidance for the management of collection or interdiction assets. Consideration is given to the same factors identified under the planning and directing section of the police information collection plan: what, where, when, why, and who.

4-7. Once the priorities have been established, a collection plan is prepared based on the CRIMINT requirements, available collection assets, and other factors including time and self-protection.

COLLECTING AND RECORDING

4-8. The collection process is the gathering of police information from all available sources. This includes raw data obtained by ALE personnel or significant data which appears substantive enough to

merit further investigative efforts. Such data may or may not have been analyzed by other law enforcement intelligence agencies. The collection effort occurs at all levels and across the full spectrum of tactical and nontactical environments. To be most effective, however, the collection effort must be planned, focused, and directed based on the CCIR and intent.

4-9. One of the most important aspects of collecting and recording police information is complying with laws and regulations. Some of the most important laws affecting CRIMINT analysts are *EO 12333*, *DODD 5200.27*, and *AR 525-13*. These laws and regulations are designed to protect the rights of citizens and police information collectors. The best legal source a CRIMINT analyst has is the SJA. [Chapter 2](#) describes the laws and regulations that are applicable to ALE personnel.

4-10. ALE personnel uses the PDP as a means of collection. Police information and CRIMINT that may impact the mission can be quickly and effectively gathered by focusing on the NAI. The PDP is used to—

- Synchronize the CRIMINT requirements with the collection efforts by prioritizing the collection tasks.
- Assign ALE and security assets for collection and interdiction coverage (patrols, checkpoints, access control points, and so forth) with emphasis on NAIs, MEVAs, HRTs, or other designated areas.
- Manage collection assets.
- Provide any special instructions to the collection assets.

4-11. In the collecting and recording phase, specific tasks must be completed. These tasks are discussed in the following paragraphs.

Determine the Requirements

4-12. This task includes identifying such things as NAIs and suspected vulnerability points, locations, facilities, and people. People may include businesses or groups and organizations of people. When focusing on criminal investigations, collection efforts related to people may require developing additional probable cause.

Identify the Assets and Resources

4-13. Collection assets and resources include available human resources, equipment, budget, and other resources or collection capabilities that can be directly or indirectly accessed to support the police collection effort. Collection assets include law enforcement sources that use overt, covert, and open or nonopen sources (described in [Appendix G](#)).

Apply the Collection Plan

4-14. When CRIMINT analysts apply the brigade or battalion staff's or the PM's collection plan, they focus on what was requested. The analysts' focus on how the police collection effort will be accomplished and considers the information collection requirements, the available assets, and the CCIR. The CRIMINT analysts are able to decipher what information must be analyzed in order to meet the commander's intent and what information should be passed through other channels to expedite support to the commander, the staff, or the PM. A collection plan that does not provide relevant, timely information to the commander is weak at best.

Specify Criminal Intelligence Analyst Tasks

4-15. In this task, individual and team responsibilities are identified. Each team member should know his role and the roles of others. When individuals know how their roles contribute to the overall plan, they are better equipped to support it. Collection responsibilities are tasked based on the ability of the CRIMINT analyst to successfully gather and analyze the assigned information.

Report and Process Police Information Into Data Streams

4-16. This information/intelligence can be varied in content, substance, and form and may originate from a myriad of sources, such as field interview cards, military police reports, CID investigation reports, and other reports obtained from other agencies.

Manage (Track) the Collection Effort

4-17. Part of managing the collection effort is ensuring that CRIMINT analysts know their collecting and recording responsibilities. The most predominant and effective aspect of this task is managing the information as it is reported. A delay in managing information can cause confusion and possibly delay relevant information from getting to the commander or PM in a timely manner. This delay may cause a "domino effect," creating an impact on the IPB, the MDMP and, ultimately, the CCIR. Incorrect information may be the direct result of inadequate information management. One of the last measures a CRIMINT analyst takes when managing information is to brief the ALE personnel involved in the collection efforts as to what happens to the information they collect. In the reporting aspect of this phase, the CRIMINT analyst ensures that resulting CRIMINT is put into the production stream or, when applicable, back into the data stream (see [Figure 4-2](#)). The police intelligence process is divided into three phases. The phases are described as follows:

- Phase 1, Common Training. Focuses on collecting and reporting information and is taught during Military Police Officer Education System (OES)/Noncommissioned Officer Education System (NCOES) instruction as part of the PIO function.
- Phase 2, Specific Training. Focuses on processing and analyzing information and is taught during specific Military Police OES/NCOES blocks with emphasis on link, pattern, and case analysis.
- Phase 3, Special Training. Focuses on analytical software and is used for intelligence analysis and production.

Receive the Information

4-18. This task identifies who will receive the information and determines the actual process or procedure for collection personnel to report information. Reporting procedures include the reporting channels for those efforts. Most often, the reporting channels are established by the commander directing the police information collection effort.

Distinguish Between Information and Intelligence

4-19. During collection efforts, raw information and CRIMINT may be collected from different sources. Regardless of the source, the CRIMINT analyst reads and reviews all data to determine its immediate value in the analysis process or its impact as CRIMINT, which may not require additional analysis.

Record the Information

4-20. Recording consists of systematically cataloging the information. At a minimum, recording defines the source, subject, and the time and date the information was collected. Recording information can be performed by writing it down or by entering it into a database system. Databases are briefly described at the end of this chapter. The information is recorded by the CRIMINT analyst. If the information later becomes CRIMINT, it is provided to the S2 and/or the DES and PM for action when OCONUS. When in CONUS, due to the restrictions placed on information gathered on US citizens, CRIMINT must be provided to the S3 and/or DES and PM for further action.

PROCESSING

4-21. Police intelligence processing occurs at set points to reduce raw data into manageable portions for analysis and production. Processing involves an initial evaluation to ensure that the police intelligence is valid, reliable, and sufficient. During processing, police intelligence information is prioritized according to

current collection and production requirements. During processing, police intelligence information managers—

- Prioritize incoming data according to collection and production requirements.
- Organize police intelligence by category, such as crime or threat, and by particular product or user.
- Enter the information into databases.
- Collate actionable police intelligence information into interim products.

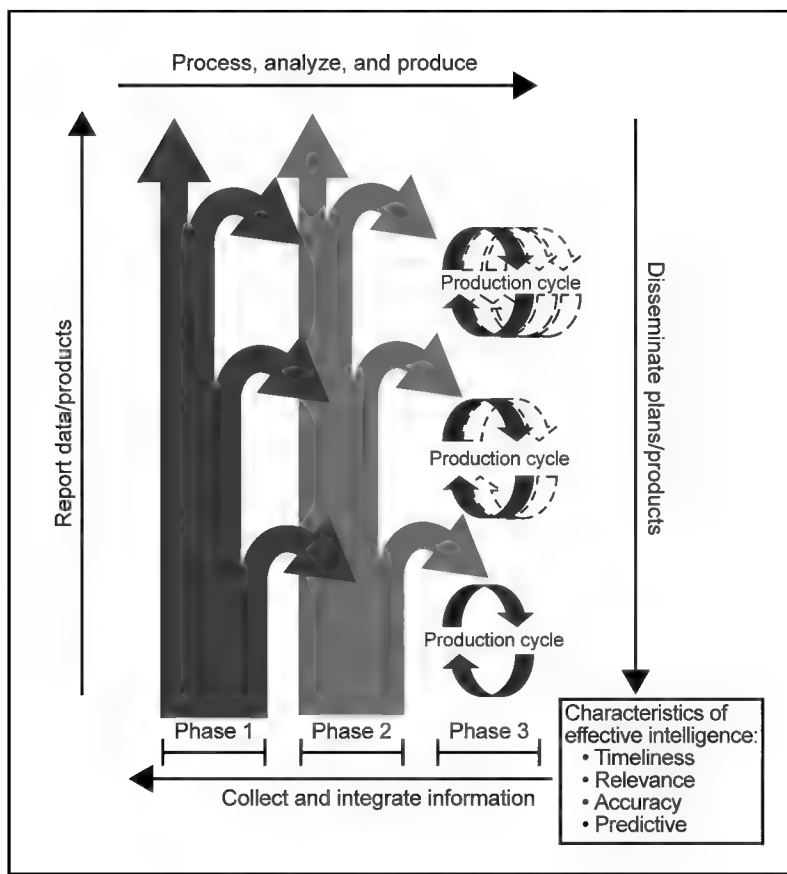


Figure 4-2. Police Intelligence Process Model

ANALYZING AND PRODUCING

4-22. In this phase of CRIMINT analysis, police information and raw data are converted into CRIMINT. Analysis is based on CRIMINT and requires the CRIMINT analyst to have all the available information to date in order to develop viable COAs (predictive analysis) for the criminal threat(s). Unlike the staff that identifies the COA for the mission during the IPB, the CRIMINT analyst determines the COA that the criminal threat is likely to take (hence predictive analysis), in order to identify possible counter-COAs. It is in this phase that the CRIMINT analyst develops hypotheses to prove or disprove the meaning of police information. This analytical process continues throughout CRIMINT analysis. During this phase, CRIMINT analysts ensure that they have a clear understanding of the commander's, DES's, and PM's intent and CCIR. All police information is viewed in relation to what the commander, DES, and PM want to accomplish. The analysis and production phase includes the following:

- **Evaluation.** The relevancy, reliability, and timeliness of police information are determined during evaluation. Information may seem irrelevant during initial evaluation; however, it should be indexed, queried, and periodically reviewed for future analysis. When reevaluated, this

fragmentary information may help define the bigger operational picture. Part of evaluating police information includes determining whether the information is relevant to the CCIR. Additionally, it must be determined whether the police information is reliable as it is presented or whether additional confirmation is required. Lastly, it must be decided if the police information is timely.

- **Integration.** How police information fits into the commander's operational picture is determined during integration. The CRIMINT analyst also determines whether pieces of police information are related to each other. As police information continues to be collected, reported, recorded, and analyzed, the bigger picture begins to emerge, and as the police information is analyzed and integrated with other police information, interpretation begins. Integrating police information in tactical plans exploits the intelligence gathered, thereby promoting emergence of the bigger operational picture.
- **Interpretation.** The interpretation of police information stems from the analysis this information and the hypotheses resulting from that analysis. During this phase, CRIMINT analysts must be open-minded to interpretation, willing to consider alternative hypotheses, and mindful of what is not known.
- **Preparation.** Preparation is the final stage of analysis that results in the production of CRIMINT products. This culminates in the final phase of the CRIMINT process dissemination and integration.

DISSEMINATING AND INTEGRATING

4-23. Preparing CRIMINT products results in the dissemination and integration of those products. CRIMINT analysts must identify the users of the CRIMINT products well in advance in order that the right products get to the right people at the right time. Generally, the users are the individuals who initiated the CRIMINT requirements and those whom they have further identified as needing the products.

4-24. CRIMINT analysts must also determine what method will be used to disseminate the CRIMINT products. Methods of dissemination may vary from such tools as military police reports and CRIMINT bulletins to threat assessments, information briefs, and so forth. See [Appendix B](#) for sample CRIMINT products. Regardless of the method used, CRIMINT analysts must ensure that the products are delivered to the appropriate users when, where, and in the proper form needed. The dissemination of timely and relevant CRIMINT products is most valuable to the user.

4-25. Dissemination occurs at several levels and is entered in the data stream for continued analysis, when applicable. Oftentimes, when the CRIMINT products are delivered, additional police information collection requirements are identified.

Note: Local police intelligence files may be exempt from certain disclosure requirements by *AR 25-55* and FOIA. When a written extract from local police intelligence files is provided to an authorized investigative agency, the following will be included on the transmittal documents: THIS DOCUMENT IS PROVIDED FOR INFORMATION AND USE. COPIES OF THIS DOCUMENT, ENCLOSURES THERETO, AND INFORMATION THEREFROM, WILL NOT BE FURTHER RELEASED WITHOUT THE PRIOR APPROVAL OF THE INSTALLATION PROVOST MARSHAL.

EVALUATION AND FEEDBACK

4-26. This function within the CRIMINT analysis process helps determine whether or not the requested information was provided and whether or not it supports the PIR or CCIR. The evaluation and feedback function also acts as a type of quality control. If the information provided was inadequate or insufficient for the requestor, the CRIMINT analyst will conduct the necessary research and analysis again based on the updated criteria provided by the requestor. The evaluation and feedback function helps requestors refine their requests and the CRIMINT analysts refine the scope of their research and analysis. When the

information meets the needs of the requestor, the CRIMINT analyst can catalogue it for possible future use, thereby amassing an organizational library of successful practices.

4-27. *Figure 4-3*, page 4-8, reflects how a military police battalion staff in support of OIF in eastern Baghdad effectively planned for and executed the PIO function. The command allowed only military police investigator personnel or Reid Interrogation Course graduates (or equivalent) to conduct the initial interviews. This is not a necessary requirement of PIO in that all ALE personnel are trained to conduct field and initial interviews. This requirement was the result of a command decision. Using all available ALE assets would maximize the results of the police information collection effort. It is critical that commanders and leaders ensure that their Soldiers do not interrogate detainees in enemy prisoner of war (EPW)/detainee operations. This responsibility must be relinquished to MI according to established regulations, as necessary.

4-28. Where specific criminal threats exist, the battalion can organize a separate PIO team responsible for collecting, analyzing, and reporting information as it relates to criminal activity within the battalion AOR. The PIO team—

- Investigates criminal offenses of coalition forces and local nationals within the battalion AOR.
- Tracks criminal investigations.

DATABASES

4-29. Advances in database technology, combined with an explosion in information sharing and networking among police agencies, has resulted in the development and expansion of these robust information repositories. ALE personnel continue to access the National Crime Information Center (NCIC) database, but can also turn to databases containing fugitive information from corrections systems and terrorist threat information from Homeland Security (HLS) and FBI systems. DOD proprietary automation systems such as the Centralized Operator's Police Suite (COPS) Information Management System and the Army Criminal Investigative Information System (ACI2) greatly improve interoperability and eliminate seams that criminal and other threats might otherwise exploit.

4-30. Access to local, theater, DOD, non-DOD, and commercial databases allow analysts to leverage stored knowledge on topics ranging from basic demographics to order of battle information. A validated DIA customer number (acquired by the joint intelligence section (J2), G2, and S2) in combination with a Secret Internet Protocol Network (SIPRNET) and Joint Worldwide Intelligence Communications System (JWICS) connectivity establishes access to most of the databases online. The challenge for an analyst is to gain an understanding of the structure, contents, strengths, and weaknesses of the database regardless of the database type. Additionally, the procedures are often difficult for extracting portions or downloading and transferring the database to unit level automated information systems.

4-31. Each intelligence discipline has unique databases established and maintained by a variety of agencies. Database access is accomplished through unit or agency homepages via SIPRNET (Intelink-S) and JWICS (Intelink).

CENTRALIZED CRIMINAL INTELLIGENCE ANALYTICAL SUPPORT ELEMENT AND DATABASE

4-32. The Centralized Criminal Intelligence Analytical Support Element (CIASE) and database are reach-back capabilities that enhances the ability of ALE personnel to readily maintain and access police information and CRIMINT. With the advancements in digital communications and centralized computer databases, the implementation of a CIASE and database would greatly support deploying commanders.

The battalion organized the PIO team as a separate section of the battalion S2 section. The PIO team was responsible for collecting, analyzing, merging, and reporting intelligence information as it related to criminal and combat activity within the battalion AOR. The battalion PIO team— • Investigated criminal and combat offenses involving coalition forces and local nationals within the battalion AOR. • Acted as the spearhead in creating targeting packages at the battalion level from actionable intelligence. • Tracked detainee activities and criminal investigations for the command. • Compiled CRIMINT for the development of criminal activity patterns within the battalion AOR in concert with the battalion S2. • Established liaison with other agencies, such as the Defense Criminal Investigative Services (DCIS), FBI, CIA, Defense Intelligence Agency (DIA), National Security Agency (NSA), and the maneuver tactical human intelligence team (THT). The battalion allowed only military police investigators or Reid Interrogation Course (or the equivalent) qualified personnel to conduct an initial interview with full interrogation responsibility being relinquished to MI according to established regulations, as necessary. The battalion established several PIO products and tools to assist in the PIO function, some of which included the following:	
PRODUCTS	TOOLS
Databases. These databases supported crime-related queries and Iraqi police blotter analysis.	PIO reports. These reports consisted of numerous types of reports that documented interviews and interrogations, resulting CRIMINT, prisoner accountability, and prisoner apprehensions and transfers.
Blotter overlay. This overlay depicted reported crimes.	Map overlays. These overlays consisted of two types of overlays. The criminal incident overlay plotted all substantiated information to provide a quick reference of evolving crime trends within the battalion AOR. This overlay was updated daily and maintained per month. The active investigations overlay plotted active law enforcement investigations within the battalion AOR.
Detainee tracker spreadsheet. This spreadsheet enabled the tracking and apprehension of Iraqis committing crimes against or attacking coalition forces and local nationals.	
PIO informant report. This report was generated after every initial interview from walk-in informants to provide for continuity in repeat informants.	Targeting packages. These packages were prepared within the concepts of the IPB with considerations to observation and fields of fire, avenues of approach, key terrain, obstacles and movement, and cover and concealment (OAKOC) and contingent upon METT-TC. The packages included such things as digital photos depicting the target from all avenues of approach, aerial imagery of the target's location depicting the surrounding area, and sketches depicting the target area.
PIO informant summary. This summary consolidated PIO informant reports, which were published and sent to adjacent battalions, maneuver THTs, and higher echelons.	
Association matrix/link diagram. The matrix and diagram were made available to identify criminal organizations/gang members.	

Figure 4-3. Sample of Planning for and Execution of PIO Functions

CENTRALIZED CRIMINAL INTELLIGENCE ANALYTICAL SUPPORT ELEMENT AND DATABASE FILES

4-33. Today when commanders deploy to operational areas, there is a lack of CRIMINT/law enforcement databases. A database must be established to assist commanders in developing the criminal threat picture. The establishment of a CIASE and database within the different operational areas would fill that void. The files would consist of—

- Intelligence obtained from previous operations.
- Spatial analysis (crime maps).
- Source operations information (data regarding sources).
- Current and previous investigative efforts with a possibility for the departing unit's suggestions for follow-on investigations.

4-34. These files support the commander, enhance the analytical capability of analysts in the field, and provide historical CRIMINT operational files. CIASE helps prevent the possibility of fostering corruption. Consider the following situation: A criminal passing as a source is willing to assist ALE personnel. The question is what is the source's motivation? Is this person—

- Using his position to gain operational information?
- Attempting to misdirect ALE personnel?
- Attempting to update local criminal groups regarding ALE agency targets of interests, ongoing investigations, or military operations?
- Selling information to ALE personnel that is of little or no use?

4-35. When a CIASE and database are established and left in place, the above type of source would be discovered and excluded. The source's information would be maintained in the database advising the new unit of his motives. Likewise, if a source was producing good information, that information also would be stored. The database would allow newly arriving units to verify, develop, and use sources and would also provide the information necessary to alert MI regarding a source.

ADDITIONAL USES

4-36. The use of a CIASE and database enhances crime-mapping capabilities. As units update information in their respective databases, the CRIMINT analysts are able to produce an overview of the criminal activity in each sector and in the operational theater. This crime-mapping capability provides a relevant criminal threat picture in a limited period of time. It also allows the CRIMINT analyst to manipulate the information quickly to keep the criminal threat picture current.

4-37. The database and the analyzed police information, would work in direct support of the IPB process for an incoming commander. Additionally, a commander could use the information to determine the specialized training needs of his Soldiers (such as additional military police investigator CRIMINT analysis training) prior to deployment. The use of a CIASE and database in deployments are rare. If CIASEs and databases were implemented, they would save commanders and the collectors and analyzers of police information and CRIMINT valuable time, producing valuable police information and CRIMINT products.

POLICE RECORDS MANAGEMENT

4-38. Intelligence information files will be maintained by the CRIMINT manager, who will keep them separate from other investigative files in the office and control access to them. The following files, at a minimum, will be maintained where a CRIMINT manager has been appointed:

- *DA Form 2804, Crime Records Data Reference.*

Note: *DA Form 2804* is a multicopy form designed to be used as an input document to the intelligence process. This form can be used to input data into a manual retrieval system and serve as a cross reference or index card.

- Raw data.
- Significant data and target analysis.
- Criminal alert notices.
- CRIMINT reports.
- CRIMINT bulletins.

Note: When there is matching or similar information, the CRIMINT manager and the operations officer SAC will review the form(s) to determine what action to take.

This page is intentionally left blank.

Chapter 5

Police Intelligence Operations in Urban Operations

Today military operations are conducted in a dynamic, multidimensional, and increasingly interconnected global OE. The world situation is complicated and split into many different factions with many possible conflicts. Different threats require intelligence operations to adapt to the ever-changing OE. Commanders plan for and continually assess the security of their forces operating in high-threat areas and constantly review protection measures. Detecting asymmetric threats' methods of operations requires a higher level of situational understanding, based on continuous intelligence support. These threats drive the need for predictive intelligence based on analysis of focused information from law enforcement, intelligence, and security activities. Establishing a robust police information collection effort that can determine the intentions and capabilities of the criminal and/or terrorist threat can greatly enhance FP for Army forces operating in high-threat areas.

Transnational groups and nonstate actors conduct a range of activities that threaten US interests and citizens at home and abroad. Such activities include terrorism, illegal drug trading, illicit arms and strategic material trafficking, international organized crime, piracy, and deliberate environmental damage. Additionally, ethnic disputes, religious rivalries, and human disasters contribute to huge refugee migrations. These further the threat to the environment and a region's stability. Collectively, these transnational threats may adversely affect US interests and possibly result in military involvement.

URBAN THREATS

5-1. Of all the environments in which to conduct operations, the urban environment confronts Army commanders with a combination of difficulties rarely found elsewhere. Its distinct characteristics result from an intricate topography and high population density. The topography's complexity stems from man-made features and supporting infrastructure superimposed on the natural terrain.

5-2. As the strategic environment has become less stable, more uncertain, and more dangerous, Army and joint forces must continue to train to address urban threats. These threats range from regional conventional military forces, paramilitary forces, guerrillas, and insurgents to terrorists, criminal groups, and angry crowds. UO require ALE personnel to provide in-depth coordination with international, national, and HN law enforcement, security, and intelligence organizations.

URBAN INSURGENTS

5-3. As urban migration increases in the developing world, rural guerrillas appear to follow. This transition of insurgencies from rural to urban areas occurs because urban areas offer a rich field of targets for insurgent attacks. People immediately notice any disruption of urban infrastructure, which results in great propaganda value. A concentrated urban population is often more susceptible to propaganda and political organization. Insurgents can easily arrange mass demonstrations using available communications facilities, both overt and covert. Travel is effortless and large urban populations provide cover and concealment. Urban areas provide a fertile environment for guerrillas to apply their rural insurgent

strategies. However, even with a rural-based insurgency, operations in urban areas offer distinct opportunities to disrupt, discredit, and demoralize the government.

5-4. The crime-conducive component of POLICE, described in *Chapter 1*, contributes to the collection efforts affiliated with civil areas, structures, capabilities, organizations, people, and events (CASCOPE) that CA personnel perform. Under CASCOPE, CA personnel collect information on the criminal environment. However, the collection efforts lack the definition as to what the contributing factors are for the criminal sanctuary to exist. The crime-conducive component provides this connectivity. When the three variables of a specific resource, a particular location, and an enforcement gap are present, they represent I&W of criminal activity. More specifically, they represent the existence of crime-conducive conditions in the AO, providing military police planners with a clearer picture of what and where the threat is.

OTHER THREATS

5-5. Some threats in underdeveloped countries may not be considered as conventional threats or insurgents. These threats may consist of such groups as personal armies of warlords (as in Somalia), organized criminals, groups of thugs loosely organized under the control of an individual (as in Haiti), or the local police force.

5-6. A characteristic of many recent stability operations has been the deterioration or complete collapse of political authority in the country or urban area in crisis. In some cases, warlords have attempted to fill the power vacuum. These individuals often have no particular claim to legitimacy. Their power comes from their weapons, not from their political skills, human services provided, or popular consent (although they must have some popular support to remain in their relative position of authority).

5-7. Organized criminal groups have become common in urban areas. They have also become an important part of the urban social structure (gangs for example) and can exert considerable influence on governments, people, and military forces conducting UO. Some large criminal organizations relying on international connections often have better resources and equipment than their insurgent counterparts. Their large financial resources, long-reaching connections, and ruthlessness provide them with the means to corrupt or intimidate local officials and government institutions. In any operation, but especially stability operations, they may violently confront and oppose Army forces during mission execution.

5-8. The tactics of urban criminal groups parallel those of insurgents. They have developed an intuitive cultural understanding of slum neighborhoods and the ability to lure civilians into criminal activities. They have also mastered the management of mobs. They recruit teenagers and young adults in their efforts against rivals and authorities, just as insurgents muster armies from the youth of rural villages. In many developing nations, there exists an alliance between insurgents and organized criminal groups. In these alliances, the insurgents defend the criminals and the criminals fund the insurgents. During many UO (particularly during or following combat, civil disturbances, or large natural disasters), organized or unorganized looting may become a critical concern. Therefore, UO may often require a combined law enforcement and military response.

5-9. When Army forces work closely with local law enforcement agencies, commanders may not need to assess the effect of street patterns on the assignment of boundaries. Instead, commanders may assign boundaries overlaid on existing administrative boundaries used by the local law enforcement agencies to increase interoperability and aid in unity of effort.

5-10. Not all criminal groups are a threat to military operations. Most criminals are only interested in money and not in interfering with friendly forces. However, groups and individuals can be influenced into assisting either the friendly or opposing force. People will also act opportunistically, shifting support and alliances as perceived advantages arise. Even seemingly law-abiding members of the urban society may conduct themselves in unexpected ways given the right conditions (coercion, threats, or bribes). These changes in behavior and attitude must be detected early, before belligerents and insurgents gain control and align civilian interests and intentions with their own.

5-11. The potential for asymmetric threats puts a premium on IPB and the other intelligence tasks, to include performing situation development and conducting PIO. The goal is to provide I&W for the commander. Operational success requires identifying enemy (criminal/terrorist) modus operandi (MO), capabilities (strengths and vulnerabilities), intentions, and COAs.

ARMY LAW ENFORCEMENT IN URBAN OPERATIONS

5-12. Urban environments are conducive to a full range of serious criminal activities. In fact, during smaller scale contingencies or stability operations, serious crime may be formally designated as a destabilizing factor to a safe and secure OE. Under such conditions, ALE personnel may provide the lead for targeting, collecting information on, and interdicting a broad range of criminal and terrorist threat activities. ALE personnel operate in close contact with local nationals daily, while patrolling, responding to incidents, operating TCPs and checkpoints, and/or conducting interviews.

5-13. If used correctly, police information collection efforts can complement the intelligence collection process (especially HUMINT), which is necessary to understand the dynamic societal component of the urban environment and detect significant change.

5-14. Urban areas transitioning from war to stability operations may also be characterized by a large surge in the number of civilian law enforcement and security agencies such as United Nations (UN) civilian police, UN border police, or the Organization for Security and Cooperation in Europe. These agencies provide an important service during the transition from conflict to postconflict by—

- Assisting HN law enforcement personnel to develop and train new law enforcement agencies.
- Providing legal oversight for the adjudication of preconflict crimes.

5-15. ALE personnel can assist US military forces, HN police, and international law enforcement agencies by providing continuity during and after the transition from military to civilian law enforcement primacy. ALE personnel can develop police intelligence networks to assist UN and HN law enforcement in gaining situational awareness and assessing, targeting, and interdicting threats. USACIDC may assist civilian law enforcement agencies by consulting with them on investigations, forensic recovery, threat trends, or security assessments. ALE networks also provide US forces with police information regarding ongoing UN or HN police intelligence, investigations, and law enforcement operations.

5-16. PIO can help synchronize international and HN law enforcement operations with those of maneuver commanders. By leveraging their police networks, ALE personnel provide liaison, guidance, and training to maneuver commanders and their staffs on legal implications associated with transitioning to civilian law enforcement. This may include identifying and articulating probable cause for search and seizure, preparing intelligence to apply for warrants, or recovering evidence. See [Chapter 7](#) for information on PIO networks, forums, and fusion cells.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD IN URBAN OPERATIONS

5-17. The IPB process remains unaffected by urban areas (see *FM 34-130*). Although complex and difficult to penetrate with many intelligence collection assets, the terrain is the most recognizable aspect of an urban area. The internal space further challenges command, control, and intelligence collection activities and increases the combat power required to conduct UO.

5-18. A primary goal of any IPB is to accurately predict the threat's likely COAs, which may include political, social, religious, informational, economic, and military actions. Commanders then can develop their own COAs that maximize and apply combat power at decisive points. Understanding the decisive points in UO allows commanders to select objectives that are clearly defined, decisive, and attainable. Decisive points may include key structures or systems used by threat forces.

SITUATIONAL UNDERSTANDING

5-19. Commanders and their staffs may be unfamiliar with the intricacies of the urban environment and more adept at thinking and planning in other environments. Therefore, without detailed situational understanding, commanders may assign missions that their subordinate forces may not be able to achieve. As importantly, commanders and their staffs may miss critical opportunities because they appear overwhelming or impossible (and concede the initiative to the threat). They also may fail to anticipate potential threat COAs afforded by the distinctive urban environment. Commanders may fail to recognize that the least likely threat COA may be the one adopted precisely because it is least likely and therefore may be intended to maximize surprise.

5-20. Adversaries will also seek to shape conditions to their advantage. They will try to change the nature of the conflict or use capabilities that they believe will be difficult for US forces to counter. They will use complex terrain, urban environments, and force dispersal methods similar to those used by the North Vietnamese, Iraqis, and Serbs to offset US advantages.

COORDINATION

5-21. Commanders coordinate their planning and efforts (early and continuously) to ensure that their decisive, shaping, or sustaining operations are not working against the efforts and operations of other agencies that may have the lead role in the operation. A critical shaping operation may be to establish the coordination to help develop a common purpose and direction among agencies.

URBAN TERRAIN

5-22. Although intricate, understanding the urban terrain is relatively straightforward in comparison to comprehending the multifaceted nature of urban society. UO often require Army forces to operate in close proximity to a high density of civilians. Even evacuated areas can have a stay-behind population in the tens of thousands.

5-23. This population's presence, attitudes, actions, communications with the media, and needs may affect the conduct of operations. Homogeneity decreases drastically as the size of the urban area increases. Commanders must take into account the characteristics of a population whose beliefs and interests may vary. Civilian populations continually influence, to varying degrees, operations conducted in an urban area. Commanders must understand cultural differences. PSYOP, CA operations, and the use of the media can greatly contribute to stability and success in UO.

5-24. Thoroughly understanding these societal aspects and avoiding "mirror-imaging"—overlaying one's own values and thought processes on top of the person or group one is trying to assess—will help to accurately anticipate civilian actions and responses.

URBAN INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE

5-25. Commanders at all levels require accurate and timely information to conduct assessments for successful UO. This is critical to planning and execution. Senior commanders have a large role in coordinating the urban ISR effort. National strategic sources (as well as open sources) may provide some of the information that commanders and staffs require on the characteristics of the human dimension, the physical properties of the terrain, and the infrastructure. However, tactical forces conducting deliberate R&S can best obtain the required information. The general characteristics of these aspects of the urban environment do not change drastically over time, with one exception—military operations or natural disasters can change the physical characteristics of the urban environment drastically.

5-26. Analysts can obtain crucial information through diligent research of intelligence databases and open sources. However, the disposition and composition of the urban threat is time-sensitive and not likely to be discovered through this type of investigation. Due to the effects of the urban environment, deceptive efforts may influence the threat more easily. R&S provide accurate and timely information regarding threat

dispositions, the composition and state of the population, and the specifics of the urban terrain. Successful UO depend on the successful conduct of urban reconnaissance.

CHALLENGES

5-27. The most significant challenge to urban ISR is the physical challenge. The organization and complexity of the urban terrain (both man-made and natural) challenge national, strategic, operational, and tactical ISR capabilities.

5-28. Commanders understand the challenges when planning and allocating time and resources to their ISR efforts. They acknowledge that subordinate commanders will face similar challenges. Therefore, commanders must consider subordinate capabilities, limitations, and needs when planning, requesting, allocating, and prioritizing ISR assets and capabilities.

RECONNAISSANCE AND SURVEILLANCE

5-29. R&S may be employed to determine the disposition, activities, and intentions of civilian populations (hostile and neutral) and uniformed or irregular threats. Reconnaissance for information collection and security continues throughout the operation. Success requires integrating all available information from civil and military sources. In foreign humanitarian assistance operations, reconnaissance helps determine how and where to effectively apply limited assets to benefit the most people. Units conducting domestic stability operations in urban environments conduct reconnaissance to help determine when and where to apply manpower and resources. Forces conducting domestic stability operations must know the legal limitations when acquiring information on civilians.

5-30. In many instances, international organizations and nongovernmental organizations (NGOs) will have been in the AOs long before US forces. These organizations produce reports, operate Web sites, and maintain databases of immense value. In the case of mines or unexploded ordnance, there is often a global positioning system reference collection of minefield survey data. US forces can access much of this information before deploying. Although commanders may access this information using intelligence operations, sound civil-military coordination may be a more effective approach.

5-31. Nonmilitary organizations can provide valuable information; however, they may resent being considered a source of intelligence. Because of the nature of their work, some organizations must remain independent and nonaligned with any military force. Commanders must foster communications and share valuable information with these organizations to become familiar with the cultures and sensitivities of the local population. Sharing relevant information is an element of information management and not ISR.

PRIORITY INTELLIGENCE REQUIREMENTS

5-32. PIR in UO, especially during stability operations, may differ from those in offensive and defensive operations. In combat operations, PIR focus on the enemy's military capability and intentions. However, intelligence collection in stability operations may be adjusted to the people and their cultures, politics, crimes, religions, economics, and related factors and any variances within affected groups of people.

INTELLIGENCE SYNCHRONIZATION

5-33. In addition to their organic assets, collection managers must be able to synchronize their collection efforts with a broad range of collection assets operating in the AO over which they have no direct control. These assets may include military police conducting PIO, USACIDC conducting CRIMINT analysis, counterintelligence (CI) and HUMINT collection teams under the control of another agency, signals intelligence and imagery intelligence collectors under the control of a joint task force, and collectors under the control of friendly elements such as the HN or coalition forces.

This page is intentionally left blank.

Chapter 6

Police Intelligence Operations on Installations

This chapter describes the collaborative relationship between the Installation Management Agency (IMA) and the DES and/or PM. It will concentrate on the DES's and PM's application of PIO on installations.

RESPONSIBILITIES OF THE INSTALLATION MANAGEMENT AGENCY

6-1. The relationships and responsibilities of IMA to regional installations are evolving. The following paragraphs serve as a guide to PIO on installations.

6-2. The IMA and some major army commands (MACOMs) have ownership of installations. Although not all inclusive, IMAs/MACOMs generally have responsibility for—

- Mobilization.
- Deployment.
- Redeployment and demobilization support.
- Training management.
- Ammunition management.
- Airfield management when applicable.
- Mission support to reserve components when applicable.
- Civil authorities and other agencies.
- Law enforcement.
- Physical security.
- Personnel security.
- Industrial security.
- Information security.
- Operational security (OPSEC).
- AT and FP planning.
- Chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE).
- Fire protection.
- Emergency services planning.

6-3. These responsibilities are delegated to designated agencies based on the function being performed. From the above list, the DES and/or PM have primary responsibility as key planners of law enforcement, physical security, industrial security, OPSEC, AT and FP planning, CBRNE, fire protection, and emergency services planning.

AUTHORITY TO CONDUCT POLICE INTELLIGENCE OPERATIONS

6-4. While the following authoritative documents do not specifically use the term "police intelligence operations," they do provide the authority and the premises on which to conduct PIO on installations. It is the police information and CRIMINT that results from the activities described in these documents that comprise PIO activities. *DODD 2000.12* directs commanders to ensure that they have a capability to

collect, receive, evaluate, analyze, and disseminate all relevant data on terrorist activities, trends, and indicators of an imminent attack. It also requires commanders to fuse suspicious activity reports from military security, law enforcement, and counterintelligence organizations with national-level ISR collection activities.

6-5. *DODI 2000.16* directs commanders to task the appropriate organizations under their command to gather, analyze, and disseminate terrorism threat information as appropriate. It requires the Army to ensure that forces are trained to maximize the use of information derived from law enforcement liaison and intelligence and counterintelligence processes and procedures. This includes intelligence procedures for handling priority intelligence requests for in-transit units and implementation of procedures to conduct IPB and mission analysis.

6-6. *AR 525-13* directs commanders to ensure that the appropriate intelligence and law enforcement organizations within their command collect and analyze criminal threat information and that the collection operations are being conducted according to applicable regulations and directives. This AR also requires commanders to ensure that threat information prepared by the intelligence community, USACIDC, PMs, and other organizations or sources be used when conducting threat assessments. See [Chapter 2](#) for further discussion of this AR, the provisions of *DODD 5200.27*, and other authoritative documents.

MANAGEMENT OF POLICE INTELLIGENCE OPERATIONS ON INSTALLATIONS

6-7. Managing PIO on installations is very similar to the description of the PIO function described in [Chapter 3](#). The distinct difference is that unlike a battalion with an S2 complemented by a full staff and possibly an assigned CRIMINT analyst, many DESs and PMs do not have a full staff available to analyze police information. The bulk of threat information generally comes from outside law enforcement and national intelligence agencies instead of organic collection assets.

STAFF RESPONSIBILITIES

6-8. The DES, PM, or SAC is responsible for the implementation and management of PIO. Effective operations are created by—

- Developing effective PIO by integrating it into management, operations, and planning.
- Providing required training and resources for PIO.
- Approving the CCIR from staff nominations.
- Providing intent for planning and directing the PIO, targeting the entity of interest, and reviewing the collection plan for compliance.
- Developing an effective law enforcement network as described in [Chapter 7](#).
- Staffing PIO activities and products with the SJA.

THREAT INFORMATION AND MODELS

6-9. Installation commanders often rely on IMA to provide threat information from DOD intelligence agencies such as the DIA, the NSA, and non-DOD agencies such as the FBI and the Department of HLS. Within the IMA, this function is the responsibility of the intelligence fusion cell. There are many organizations in the intelligence community. *FM 2-0* describes the various intelligence and law enforcement agencies that provide intelligence support to military operations and installations.

6-10. For local threat information, installation commanders rely on the DES, PM, and CID to coordinate with local, state, and federal law enforcement agencies. These personnel in these agencies can provide valuable information on local threats such as gangs, hate groups, and criminals. The installation commander counters these and other threats through physical security measures, random antiterrorism measures (RAM), access control points, aggressive law enforcement, and so forth.

6-11. Installation assets that are trained to collect and report police information and may assist in the development of threat information include—

- ALE patrols.
- Access controllers.
- USACIDC and military police investigators.

6-12. In order to capture police information and CRIMINT, the DES, PM, and CID use a threat model. Threat model designs can differ based on the type of environment within which a mission is being conducted, as well as the conflict intensity within that environment. For example, on an installation with habitual relationships and a relatively stable OE, models may, over time, reach a degree of specificity and detail not possible in the more fluid environment associated with a contingency operation. Clearly defined threat categories are essential to the development of a threat model.

6-13. Intelligence managers must define in detail each threat group by capability and intent. For example, whereas a gang might target individuals, it does not target specific installations. Understanding what a gang targets is central to understanding the threat that gang poses to an installation. *Figure 6-1* is a sample model that was designed for use at US Army installations. It is not prescriptive, but is descriptive of the need for a standardized quantifiable method to conduct threat estimates. The police information and CRIMINT collected from PIO efforts are put into databases. These databases are described in *Chapter 4*.

1 Threat Elements	2 Threat Analysis Factors					3 Exist Capability & Targeting Constant	4 Installation Specificity		5 Probability Factor	6 Total Threat Score
	a Exist	b Capability	c History	d Intent	e Targeting		a Indirect Threat	b Direct Threat		
2 Unsophisticated Criminals										1
3 Drug Criminals										2
4 Gangs/ Hate Groups	1	1	1				1		High +1 Significant +.75 Moderate +.50 Low +.25	3 4.25
5 Extremists										5
6 Organized Criminals							+1	x1.50		6
7 Saboteurs										7
8 Terrorists	1	1	1	1	1					8 9 10

Figure 6-1. US Army Installation Threat and Crime Model

POLICE INTELLIGENCE OPERATIONS PLANNING AND EXECUTION

6-14. During the planning and directing of PIO, the DES, PM, or SAC must identify and approve the CCIR and plan and direct the information collection effort. The DES, PM, and CID planners consider the same factors the staff identified in *Chapter 3*.

- What (activities and indicators that will confirm the threat).
- Where (probable locations to include NAI).
- When (the time that the event may occur).
- Why (justification of the requirement).
- Who (the persons and agencies needing the results of the collection efforts).

6-15. Once priorities have been established, a police information collection strategy and plan are prepared based on the same factors described in *Chapter 3*. The police information collection plan will—

- Synchronize the CCIR with the collection effort by prioritizing collection tasks.
- Assign law enforcement assets for the collection effort and interdiction coverage (patrols, checkpoints, access control points, and so forth) with special emphasis on NAI and vulnerable areas.
- Manage collection assets such as patrols, contraband detectors, access control teams; special services such as investigations, dog patrols, and physical security; or external support such as explosive ordnance disposal (EOD).
- Provide indicators and special instructions.

6-16. The police information collection process is the same for installations, with the exception of the reporting of police information and CRIMINT to S2s and G2s (see *Chapter 3*). Because of the restrictions placed on the collection of information about US citizens by intelligence agencies, police information and CRIMINT will only be channeled through S3s and G3s and law enforcement channels, except when *paragraph 1.6a of EO 12333* applies.

6-17. The remainder of PIO and its processes are performed in the same manner as described in previous chapters. A recap of those actions is as follows:

- A collection plan is used to gather police data or CRIMINT products required to answer the CCIR in the collection phase.
- The collected data is entered into a data stream through reporting and is organized and prioritized in preparation for analysis and production of CRIMINT in the reporting and processing phase.
- Data analysis, evaluation, and interpretation occur and are then converted into CRIMINT products that are entered into a production stream and on to production cycles in the analysis and production phase.
- These products are disseminated to appropriate users when, where, and in the form needed in the dissemination and integration phase.
- Evaluation and feedback occur (typically initiating more CRIMINT requirements) during all phases.

Chapter 7

Police Intelligence Operations Networking

This chapter describes the development of PIO networks in various OEs and the development and management of forums, committees, councils, and threat working groups. This chapter also describes some of the law enforcement and intelligence agencies and the tools that they can provide in support of ALE personnel.

PIO networks in tactical and nontactical environments are developed similarly with the same overarching objective—to enhance police information and CRIMINT sharing. Whether in a tactical or nontactical environment, subtle influences may create some variation in network membership from one ALE organization to the next. Influences such as the availability of agencies within the local OE, the personalities of organizational leaders, and cultural or operational differences between agencies may influence membership participation and team dynamics. For instance, ALE personnel may not have a local FBI or Bureau of Alcohol, Tobacco, and Firearms (BATF) field office within the operating vicinity of the installation. Likewise, UN civilian police may be operating in the Balkans while preparing to deploy civilian police into the Afghanistan theater. Despite such local variations, a more general perspective provides important similarities in developing and managing PIO networks that can provide a firm basis for future ALE doctrine.

By using standard protocols, ALE personnel may develop PIO networks anywhere in support of Army installations or specific AOs. Such standardization would provide a platform for tailoring staff, providing institutional training, and selecting the most appropriate resources such as automation and other emerging technologies. The successful development of PIO networks may help create seamless OEs between local agencies and may provide a springboard for developing vast regional, national, or even international PIO networks.

NONTACTICAL NETWORKS

7-1. *Figure 7-1*, page 7-2, provides a sample of a nontactical PIO network at the Army installation level. This is just a sample of one possible network pattern and would undoubtedly change from locality to locality based on the aforementioned variables. In *Figure 7-1*, ALE personnel are located in the center, with installation agencies on the right (gray background) and agencies located off the installation are located on the left (light gray background). Typical law enforcement agencies may include international, federal, state, and local law enforcement depending on whether the installation is located in CONUS or OCONUS.

7-2. Relationships between ALE personnel and other PIO network members will differ. Some network members will require day-to-day working relationships while others will be based on—

- Mutually supporting relationships for routine activities.
- Occasional collaboration.

7-3. PIO network relationships between agencies will ebb and flow based on numerous factors affecting the OE. Relationships will also continue to develop as bonds are strengthened through joint ventures and as agencies expand their own operating network.

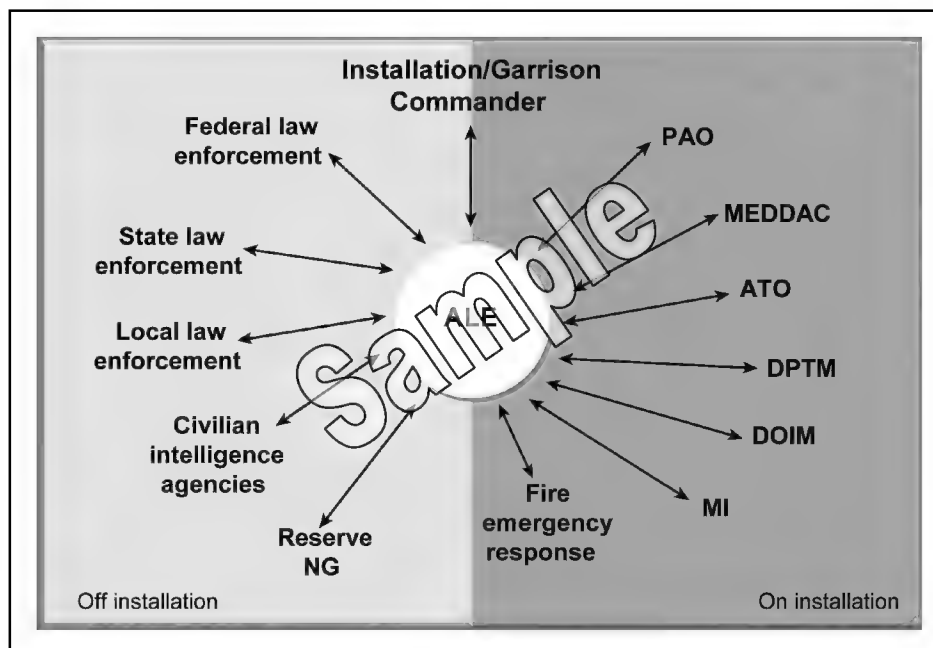


Figure 7-1. Nontactical PIO Network

TACTICAL NETWORKS

7-4. *Figure 7-2* provides a sample of a PIO network in a tactical environment. PIO networks will also vary from locality to locality in a tactical environment. Similar to the nontactical PIO network, military organizations are located on the right (gray background), while civil-military agencies are located on the left (light gray background).

DEFINING NETWORK PARTICIPANTS

7-5. A PIO network should be tailored to meet the local (common) OE and is influenced by such factors as the threat assessment, intelligence requirements, and the specific needs of participating agencies. A PIO network will generally consist of agencies located within the immediate OE. However, with a growing number of agencies using the Internet, this may not always be the case. Instead, agencies participating in a PIO network may be defined by their affiliation rather than their actual location and may be located across the state or country, or even located across the world. Such arrangements may fill essential gaps in the PIO network. If particular agencies are not represented in the local environment (for example, FBI or Drug Enforcement Administration (DEA) field offices, MI, or HN law enforcement), ALE personnel can add them to their network by either leveraging another law enforcement PIO network or making direct contact with the agency using Internet-based intelligence services.

7-6. The success of the PIO network depends on the mutual exchange of timely, relevant, accurate, and predictive intelligence with regards to established laws and regulations. To accomplish this, PIO managers must work closely with other agencies and thoroughly understand each agency to complement each other's strengths and weaknesses. They must understand each organization's vision, mission, goals, and objectives and identify and develop strategies to overcome cultural, organizational, and operational barriers. By reviewing organizational charts, PIO managers can align their organization with other organizations. They should identify and superimpose the task and purpose for each key member onto an organizational chart to assist with aligning parallel levels and similar intelligence functions between organizations. Using the modified organizational chart, managers can identify comparable staff positions and existing gaps between organizations. *Figure 7-3*, page 7-4, is a sample of an organizational chart showing nested organizations.

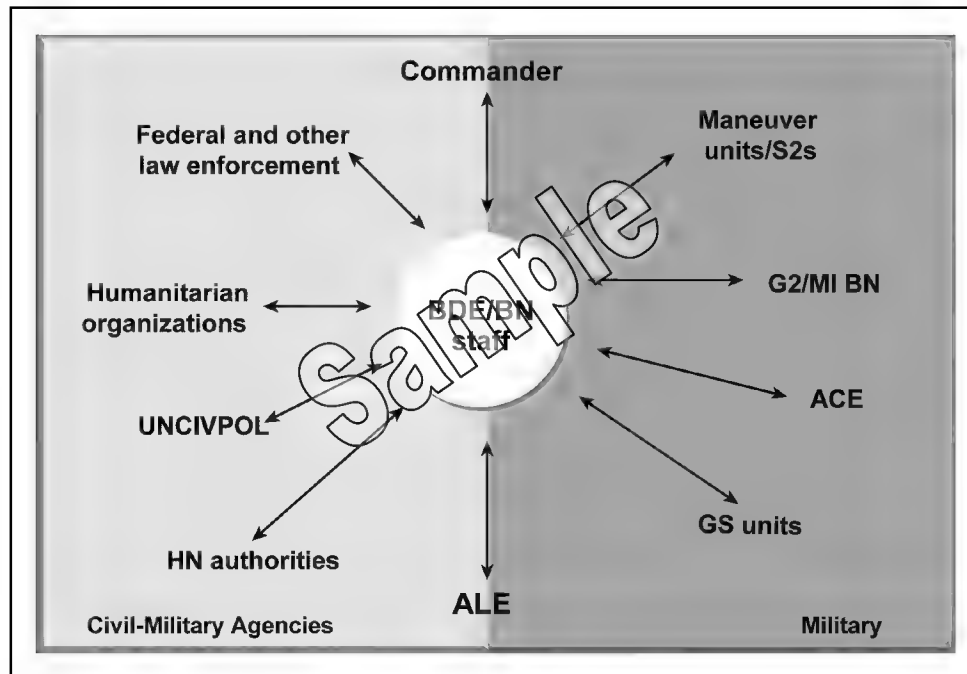


Figure 7-2. Tactical PIO Network

7-7. The modified organizational chart can now be used to identify and align intelligence contacts within each participating agency. It is important to nest appropriately similar command and staff, levels of authority, and intelligence functions between each agency to increase interoperability. For instance, ALE personnel must recognize that similar ranks or titles between organizations do not necessarily translate to the same management level. A lieutenant with the state police, for example, may be the equivalent of a military police colonel. Also, appropriate staff alignment can help to build personal working relationships for more effective interagency cooperation and intelligence sharing. When nesting organizations, PIO managers must identify and cross-level or provide training to bridge organizational gaps, to include cultural, operational, technological, and experience gaps.

7-8. ALE personnel must develop a comprehensive communications system to support a PIO network. Contact lists for all agencies should be disseminated throughout the network and routinely checked to validate less frequent contacts and maintain personal working relationships. It is desirable that agencies have compatible communications systems for routine support. Compatible communications systems should include—

- Conventional communications systems such as—
 - A telephone.
 - A radio.
 - A fax machine.
- Nonconventional communications systems such as a—
 - A Secure Internet Protocol Router Network (SIPRNET).
 - A Nonsecure Internet Protocol Router Network (NIPRNET).
 - An electronic intelligence interface, videoconferencing capability.
 - Web sites.
 - Computer databases.

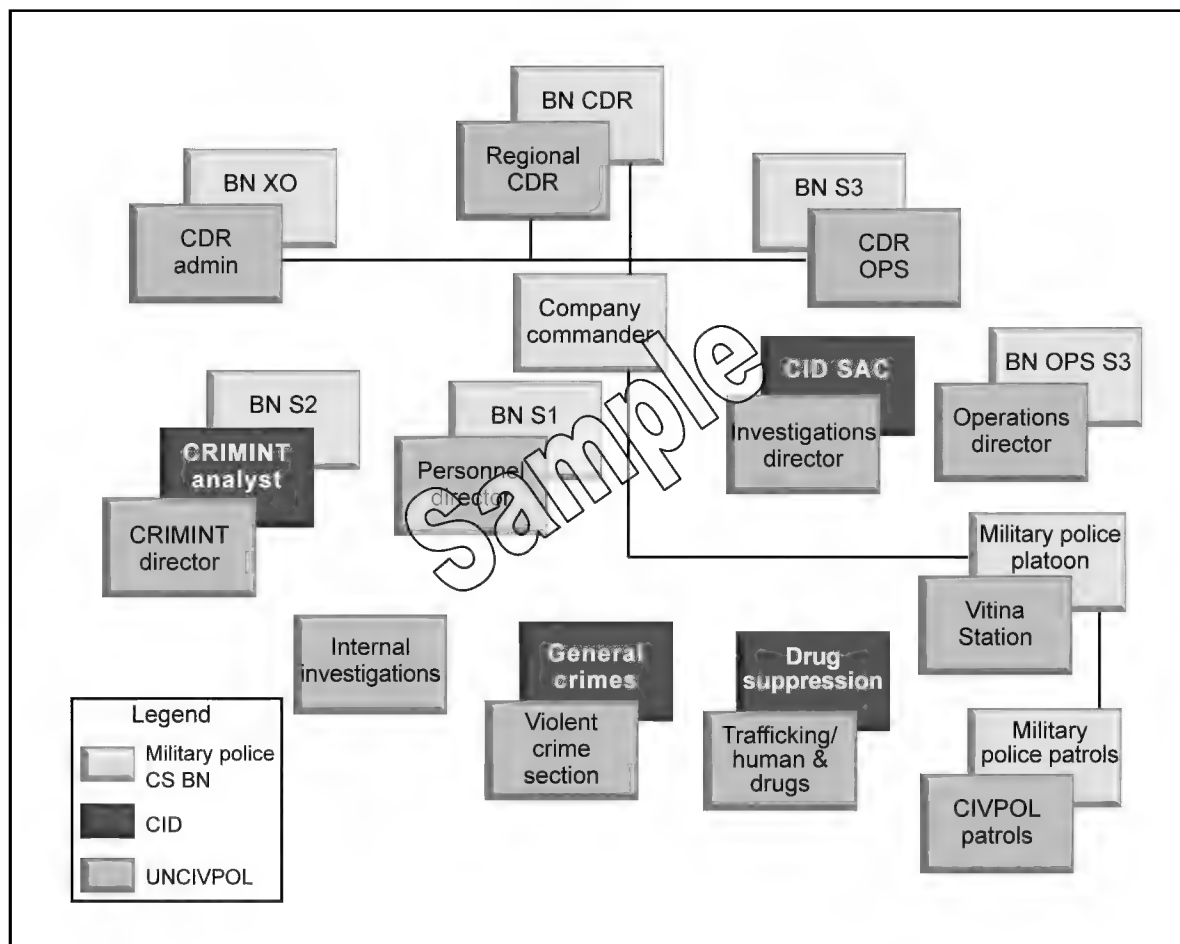


Figure 7-3. Organizational Chart

FORUMS AND THREAT WORKING GROUPS

7-9. Whether in a tactical or nontactical environment, commanders must establish forums and/or threat working groups to enhance their PIO networking capabilities. The PM should always be a member of these forums and/or cells.

DEVELOPING FORUMS

7-10. A forum is a select group of agency representatives who are usually selected from within the PIO network to meet as part of a working group, committee, council, or cell. The purpose of the forum can be to accomplish any number of objectives such as targeting, planning and directing, collecting, processing, analyzing, and producing or disseminating intelligence to meet established criteria. Each forum should have a charter that clearly defines its vision, mission, goals, and objectives. Examples might include such common forums as a gang task force, FP council, or AT working group; or they may include less common forums such as an installation threat working group or a law enforcement targeting cell. Because forums are established for different reasons, forum chairpersons will be designated based on the intent of the forum. For example, the chairperson for law enforcement concerns will most likely be the PM, the chairperson for FP concerns will most likely be the FP officer, and so forth (see [paragraph 7-16](#)). Based on their charter, forums can either be recurring or limited in scope.

Recurring Forums

7-11. Recurring forums provide a broad-based platform for sharing CRIMINT and police information and are usually formed without a specific end state. Each meeting is generally guided by an agenda focused to achieve current goals and objectives. A recurring forum may be formed to provide the latest updates relevant to its charter, or it may provide a platform for a more cyclic process such as planning, directing, and targeting.

7-12. Targeting consists of receiving raw data or information through various sources, developing actionable CRIMINT (through the CRIMINT process), and then targeting an individual or organization associated with a specific crime. An example of targeting is that of economic crimes, where an individual commits systematic larceny of government properties, such as central issue facility (CIF) items. CIF personnel report the individual suspected of committing larceny. ALE personnel initiate an investigation, develop actionable CRIMINT, target the individual, complete the investigation by proving the elements of the crime, and forward the report for the purpose of adjudication.

7-13. An AT working group and a law enforcement targeting forum are examples of recurring forums because they are focused on an ever-present challenge. These examples could continue indefinitely to meet specific objectives that are developed and refined on a recurring basis to meet changes in the threat assessment or other changes affecting the OE. Recurring forums can be challenging for ALE personnel. To be successful, such forums require a long-term commitment, membership stability, and well-prepared and focused agendas. Law enforcement targeting forums, for example, require a continual assessment of the threat, current intelligence analysis and production, and updated targeting folders prepared before each meeting.

Limited-Scope Forums

7-14. Limited-scope forums are generally brought together for a particular mission or task and would normally have a clear end state. Such forums provide an excellent platform for crisis and consequence management. For example, a task force for a homicide case is a limited-scope forum, convening for the purpose of solving a specific murder case. Once the case is solved, the forum's charter would be accomplished and the forum disbanded. While the participating agencies are no longer part of the forum, they remain part of the network and are available to participate in future forums.

TAILORING FORUMS

7-15. Whether a forum is recurring or limited in scope, membership must be specifically recruited for each particular charter. Membership should be both inclusive and exclusive. It must include all relevant members from the PIO network (such as the G2); the director of plans, training, and mobilization (DPTM); and the garrison commander, but exclude all others less relevant. Admitting too many agency representatives or those unrelated to the mission may create a forum that is either too large or too diffused to be effective. Selective membership will encourage an open dialogue, especially when sharing classified or sensitive intelligence. Law enforcement personnel, for example, may not openly share police information with non-law enforcement agencies or members present. If a forum were created to target gangs, however, it should include a representative from each agency within the PIO network with specific, relevant jurisdiction, such as local or regional gang units. Additionally, once the forum is established, membership should be guarded to minimize membership turnover or influx that can reduce the effectiveness of the group dynamics.

7-16. Forum management must also consider the appropriate membership level and functional expertise. Some forums may require managers because their charters require rapid decisions to integrate intelligence closely with operations. Targeting forums, for example, are best supported by decision makers who can make immediate operational decisions for their respective organizations. This can abbreviate the targeting cycle by cutting through the normal staffing process required for analysts to inform commanders regarding targeting results. This may be particularly important when planning and targeting joint law enforcement

operations where staff delays from each agency can compound critical time delays between actionable intelligence and taking action. Forum management should also consider the appropriate functional expertise required to accomplish charter goals and objectives during the forum. For example, a more general forum mix (such as managers, analyst, and targeters) may provide a quicker staff process, but may provide less specific intelligence than more specific representation (such as a group of analysts).

MANAGING FORUMS

7-17. Effective management is critical in achieving a level of interagency cooperation beyond a simple exchange of information. The traditional challenges of managing time, priorities, and results must be addressed at every meeting. The forum agenda, supported with the latest intelligence updates, can help manage time, while providing linkage between forum goals and objectives, and the group's current focus. A formal agenda can also provide a medium for staffing forum topics with agency management before each meeting and, when used to document results, can provide a standard product for dissemination to respective agency staffs.

7-18. Critical management positions such as a chairperson or project leader, a person or team responsible for developing the agenda and collecting current intelligence, and someone responsible for documenting forum results and preparing in-progress reviews must be selected for the forum. Because membership may represent many diverse backgrounds, forum progress can easily become sidetracked and lose focus. To counter this, it is important that the forum chairperson review agendas before meetings, maintain focus during meetings, make decisions on dissemination, and review and assign intelligence tasks to forum members. Forums must also include functionary experts for those intelligence processes being conducted, and the chairperson or forum manager must be familiar with the major function associated with the forum's charter. For example, the chairperson for a law enforcement targeting forum may not provide discrete targeting input into the agenda. However, he must understand the targeting process and be able to translate specific guidance based on input such as the current threat assessment and CCIR into targeting priorities.

THREAT WORKING GROUPS

7-19. Forums, when developed for the purpose of integrating intelligence from multiple sources, are referred to as threat working groups. These groups provide one of the most important components of an effective PIO network. Generally, they represent the most senior intelligence forum for each organization and network (for example, installation threat working groups, state or regional law enforcement threat working groups, or an ACE). A threat working group provides a central location for CRIMINT management and is used throughout the Army at different echelons in both tactical and nontactical environments. Threat working groups may be formal or ad hoc, based on specific CRIMINT, operating requirements or constraints, and available resources. Like forums, threat working groups may be staffed on a recurring basis or under a limited operating scope. They may meet periodically or operate 24/7.

7-20. Although fusion of CRIMINT may occur at any level, establishing a threat working group requires a more formal structure. A threat working group may be established at almost any organizational level that can provide the requisite direction and expertise. Threat working groups can manage CRIMINT from specific or multiple sources. They are designed to collect CRIMINT products from any number of forums, such as EOD teams working postblast analyses, AT working groups, law enforcement targeting forums, juvenile review boards, gang task forces, or any number of other forums. Additionally, they can manage CRIMINT collected directly from separate or isolated sources.

THREAT WORKING GROUP PARTICIPATION

7-21. ALE personnel must provide threat working groups or participate in local threat working groups in both tactical and nontactical environments. In the tactical environment, they should work closely with a task force ACE or other threat working groups. In nontactical environments, ALE personnel should

provide a threat working group at the PM level or, where available, work closely with the installation threat working group. The following manuals include a discussion of threat working group activities or cells:

- *AR 525-13* mandates that installation commanders, "designate a focal point to coordinate requirements for, and receive and disseminate time-sensitive threat information received from federal, state, local, HN, USACIDC, and US intelligence agencies,"
- US Army installation commanders' blueprint states, "Using the installation S2 as a base, form an installation focused intelligence threat working group including representatives from these offices: PM, CID, CI, local, state, federal, and HN law enforcement and intelligence agency representatives. If OCONUS, include supporting MI detachments and HN law enforcement and intelligence agency representatives. Meet often and disseminate aggressively."

7-22. While neither manual specifically mandates how threat working groups should manage CRIMINT, where possible, law enforcement must provide formal structure, staffing, training, and resources. Also, ALE personnel should incorporate local PIO network representatives for a more comprehensive threat picture.

THREAT WORKING GROUP STRUCTURE

7-23. Developing or tailoring a threat working group is conducted similarly to tailoring a forum. Threat working groups supporting higher organizational levels will require more formal structure, management, and resourcing. At higher organizational levels, threat working groups will be expected to manage larger volumes of intelligence data and products to service more CRIMINT forums and agencies through—

- Product dissemination.
- Planning and directing.
- Other intelligence support activities such as answering requests for information (RFIs), providing consulting services, and supporting intelligence queries. An installation, for instance, could potentially manage far more networks, agencies, and forums than one of its major subordinate commands (MSC), just as an MSC could manage more intelligence products and services than one of its subordinate units.

7-24. Threat working groups must be tailored to support projected estimates regarding the management of intelligence activities, the operating tempo (OPTEMPO), and product and service support. An analysis of threat working group requirements can be conducted similarly to that required for tailoring an organization. Although resource availability will impact threat working group operations, managers should consider the overall intelligence requirements when developing a threat working group, to include the following:

- Threat working group charter with mission, goal, and objectives.
- Expected intelligence management responsibilities.
- Number and type of agency participants.
- Expected intelligence products and services.
- Current threat and vulnerability assessments.
- Current FPCON.
- Volume and complexity of intelligence requirements.
- Targeting cycles and products.

THREAT WORKING GROUP STAFFING

7-25. A full-time intelligence or police intelligence manager is recommended for the management of a threat working group. This position may be required even during limited operations to maintain police information and CRIMINT flow, storage, query, and dissemination. In general, threat working group staffing should include a representative from each charter organization within the PIO network, but at a minimum, it should include the following:

- CID.
- PM.
- MI.

- 902d MI Detachment.
- UN, international, and coalition law enforcement agencies.
- HN law enforcement agencies.
- Federal, state, and local law enforcement, as applicable.
- Other intelligence agencies/collectors, when applicable.
- Other military installations.
- FP and AT officers.
- DPTM.

Appendix A

Integrating Police Intelligence Operations Planning in the Military Decision-Making Process

Although designed for tactical planning, the MDMP can assist in the accomplishment of any mission, including PIO. The MDMP is an established and proven analytical process that helps organize the thoughts of a commander and his staff to examine specific situations and reach logical decisions. It helps them apply thoroughness, clarity, sound judgment, logic, and experience to reach decisions and develop effective plans. Steps of the MDMP are the same for any mission. The MDMP establishes procedures for—

- Analyzing a mission.
- Developing and wargaming a COA against the threat.
- Comparing friendly COAs against threat criteria and each other.
- Selecting the best COA.
- Preparing an OPLAN or OPORD for execution.

The MDMP depicted in *Figure A-1* organizes these procedures into seven manageable, logical steps. These steps provide the commander and his staff with a means to organize their planning activities, understand the mission and the commander's intent, and develop effective plans and orders.

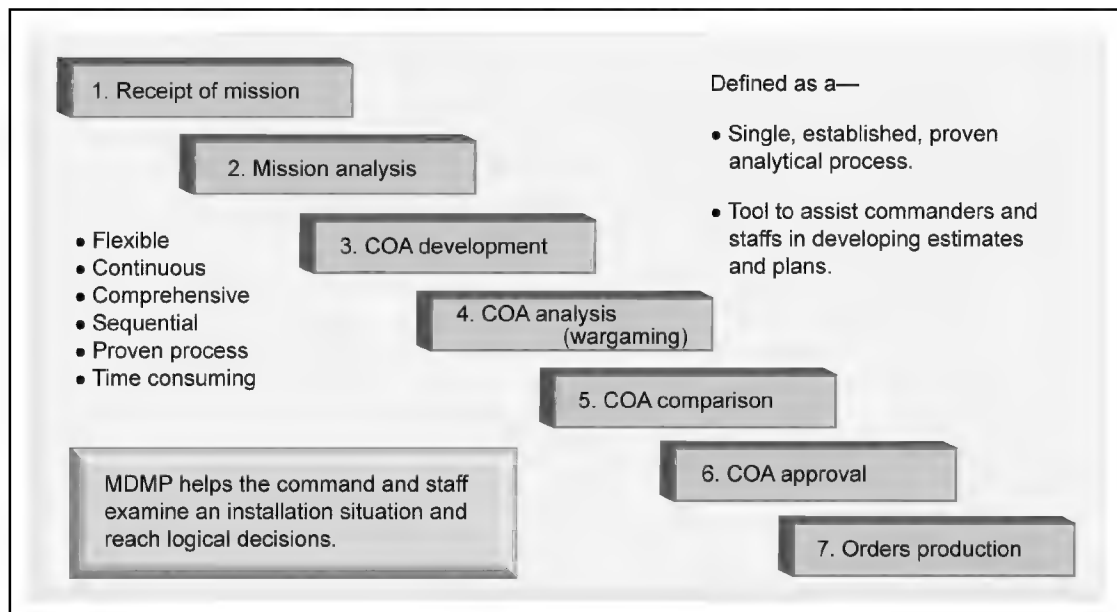


Figure A-1. MDMP

THE MILITARY DECISION-MAKING PROCESS

A-1. Interaction among various planning steps allows a concurrent coordinated effort that maintains flexibility, makes efficient use of time available, and facilitates continuous information sharing. *FM 5-0* describes the planning process and prescribes formats for staff estimates and orders.

A-2. Although the seven-step planning process is the same for all types of planning, there are unique challenges concerning the MDMP for installation commanders not found in a tactical unit. An installation is normally formed of units and functions to support the various administrative purposes of its residents and tenant units. It is not, as a rule, organized for combat operations. Installation staffs vary widely in size and capability. Some installations are assigned military and civilian staffs less experienced in the MDMP than officers in a tactical staff. The following paragraphs describe the MDMP and show how the PIO function is embedded in that process.

RECEIPT OF MISSION

A-3. *Step 1* of the MDMP begins with receiving or anticipating a new mission, such as the mission to collect police information. A directive from higher headquarters, a change in FPCON, or a specific incident (significantly increased criminal incidents in a unit area) may initiate planning. Timely notification of an impending planning session facilitates preparedness for the planning staff. In a crisis action or management situation, the following staff should be notified and should participate in the planning process:

- Local, state, and federal agencies in HN.
- Police.
- PIO network members.
- Emergency medical services.
- Installation staffs.
- Others, as identified.

A-4. Once notified of an impending planning session, staff officers prepare by updating their estimates and other critical information relating to PIO. Planners gather the necessary planning tools that will be used during mission analysis and COA development. These tools include—

- Threat estimate.
- Higher headquarters' order and plans, such as prioritized collection requirements.
- Memorandum of agreement (MOA) and memorandum of understanding (MOU) with off-post agencies.
- Maps and other terrain products.
- Applicable DA and DOD regulations, instructions, and policies.
- Installation SOP.
- Current staff estimates.

MISSION ANALYSIS

A-5. *Step 2* is mission analysis, which is the crucial step in determining the mission and developing situational understanding. It consists of 17 tasks (described in *Chapter 3, FM 5-0*), not necessarily sequential, and results in a restated mission, commander's intent, and planning guidance to the staff for COA development. Threat analysis begins during the mission analysis. A thorough mission analysis enables the commander to better understand friendly forces and capabilities, the threat, and the environment. Additionally, it assists the commander in determining the criticality and vulnerability of his assets and the areas where he will accept risk.

A-6. Mission analysis includes determining specific tasks, normally provided by higher headquarters; specified tasks, normally provided by the G2 or S2; and implied tasks, determined by subordinate planners (such as the company commander who is in receipt of the police information collection effort). It is here, when addressing PIO, that planners analyze the tasks associated with police information collection efforts.

Mission-essential tasks are derived from the list of specified and implied tasks that form the basis of the mission statement. An analysis of specified tasks will result in implied tasks.

A-7. Another part of mission analysis is determining limitations and assumptions. *AR 525-13* and the manuals identified in [Chapter 2](#) provide many of the limitations imposed on a commander regarding police information and CRIMINT collection and the authority and jurisdiction of terrorist incidents. Commanders must comply with these manuals when executing PIO actions.

A-8. The staff gathers all relevant PIO information. Where information and facts are not available, assumptions must fill the gap and provide the necessary detail to continue the planning process. However, assumptions must be pursued to verify them as fact, or they must be dismissed all together. All information and facts must be constantly reviewed for validity. Do not "assume away" problems, particularly a threat potential. New facts may alter requirements and require a reanalysis of the mission. Whenever the facts or assumptions change, the commander and staff assess the impact of these changes on the plan and make the necessary adjustments, including changing the CCIR if necessary. The dissemination phase of the CRIMINT process applies in this step—the CRIMINT analysts submit CRIMINT products to the staff for consideration in the mission analysis.

A-9. Central to the MDMP are the CCIR (inclusive of the friendly force information requirements [FFIR] and the PIR) and essential elements of friendly information (EEFI). Although EEFI are not part of the CCIR, they become a commander's priority when he states them. EEFI help commanders understand what enemy commanders want to know about friendly forces and why. These requirements and the commander's intent provide focus to the collectors in the PIO collection efforts.

COURSE OF ACTION DEVELOPMENT

A-10. *Step 3* of the MDMP begins with the staff developing COAs for analysis and comparison after receiving the commander's planning guidance. In tactical planning, planners begin COA development by analyzing the relative combat power of friendly and enemy forces. In PIO planning, this step may consist of a troop-to-task analysis. For example, matching generic units, functions, and/or assets against collection requirements will provide insight into the battalion's resource requirements and shortfalls. Planners initiate the development of and strategy for the police information collection plan in this step of the MDMP.

A-11. Another way to begin conceptualization is to use a reverse planning technique. Start with a worst-case scenario such as a high-explosive vehicle bomb detonated at the battalion's tactical operations center. In this instance, the planner first develops the COA from the reactive perspective then develops a concept of prevention and protection.

A-12. The COA will be presented to the commander for consideration in the form of a concept statement and sketch. The concept may be presented as a phased task (preincident, incident, and postincident) or as proactive and reactive tasks. The concept statement must describe the objective, the task and purpose and how they support the higher headquarters' concept, and the main effort of each task with each supportive element identified. The main effort could be by unit or more likely by function.

A-13. Since military operations can have an adverse effect on the environment and civilians commanders must consider the local community and infrastructure, as well as friendly forces. The staff assesses the hazards, develops controls, determines residual risks, and advises the commander on risk mitigation measures.

A-14. The concept statement and sketch cover the who (generic task organization), what (tasks), when, where, how, and why (purpose) for each subordinate unit and any significant risks and locations where they might occur. The sketch must include the location of—

- Response and security forces.
- Access control points.
- Possible threat infiltration locations.
- Command post and emergency operation centers.

- Evacuation routes.
- Staging areas.
- Mass casualty care facility.

COURSE OF ACTION ANALYSIS, COMPARISON, AND APPROVAL

A-15. *Steps 4, 5, and 6* of the MDMP are similar between tactical and nontactical planning. The detailed COA analysis allows the staff to refine and synchronize each COA. The procedures for conducting a wargame are found in *FM 5-0* and can be modified for PIO planning.

A-16. COA comparison starts with each staff officer analyzing and evaluating the advantages and disadvantages of each COA from his perspective. The staff then collectively compares each COA to identify the one that has the highest probability of success. There are several techniques that facilitate the staff reaching the best recommendation. The most common technique is the decision matrix, which uses evaluation criteria to assess the effectiveness and efficiency of each COA. After completing its analysis and comparison, the staff identifies its preferred COA and makes a recommendation to the commander. After the COA decision brief, the commander selects the COA he believes to be the most favorable to accomplish the mission. In the event of a PIO mission, he will select the COA that will best achieve the desired end state of PIO collection efforts. If PIO are conducted in support of a larger effort, the COA will most likely support the larger effort. The G2 or S2 or the DPTM, DES, or PM needs to nest PIO with whatever COA is chosen. The commander then issues any additional guidance on priorities, orders preparation, rehearsals, and preparations for mission execution.

ORDERS PRODUCTION

A-17. *Step 7* of the MDMP is to complete the plan and publish the order. The five-paragraph OPORD format described in *FM 5-0* is the most appropriate.

THE CRIMINAL DIMENSION

A-18. A dynamic to consider when planning PIO in conjunction with conducting the MDMP is the criminal dimension. This is not a new dynamic to ALE personnel, but rather, one that has been previously underestimated, underrepresented, and/or overlooked when conducting the MDMP for military operations. Frequently, the criminal dimension is the last priority of military police planners due to the platform-based, maneuver centric nature of the US military; an aversion to law enforcement operations in general; and the traditional military police response to supporting that nature. In the past, the criminal dimension was also neglected because of the absence of assessment tools and constructs. The acronym POLICE (described in [Chapter 1](#)) and the processes described in [Chapters 3](#) and [4](#) provide the fundamentals necessary to assist in assessing the criminal dimension. [Figure A-2](#) shows PIO criminal dimension considerations in relation to the MDMP.

A-19. The criminal dimension adds an uncertainty to the contemporary operational environment (COE). This dimension is generally unpredictable and unprovoked. The ramifications of an unchecked and unevaluated criminal dimension may result in a significant impact to the mission.

A-20. The criminal dimension is comprised of criminal threats that, when left unchecked, will impede critical tasks. Assessment of the criminal dimension is vital when considering the civil considerations of METT-TC in the initial planning phases of an operation.

A-21. [Figure A-2](#) addresses assessing the environment. ALE personnel do this through POLICE. Upon receipt of the mission (*Step 1*), the military police planner gathers all information concerning the environment and begins an in-depth analysis of the effects the environment will have on the mission.

A-22. While conducting the mission analysis (*Step 2*), the military police planner highlights facts and assumptions collected from the assessment of POLICE. The facts and assumptions highlight the "E" of POLICE and help the staff understand the effectiveness of existing criminal justice systems. The military police planner then provides intelligence requirements that will confirm the presence and degree of effectiveness of the system in relation to the mission.

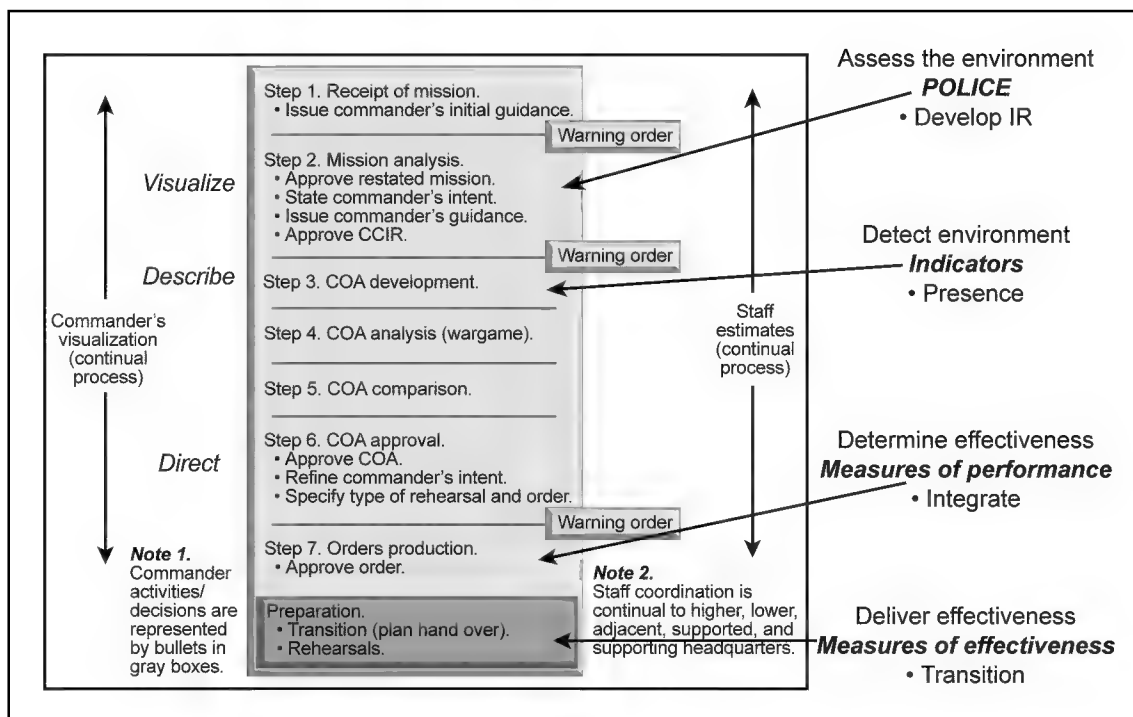


Figure A-2. PIO Criminal Dimension and the MDMP

A-23. During COA development, the military police planner identifies the indicators and synchronizes with other staff agencies the desired effectiveness the system must have in order to support the mission. If the military police planner determines that no mechanism exists or the ones present are ineffective, he emphasizes this during the mission analysis and identifies the risks if left unchecked. Areas where no enforcement mechanisms exist and the commander does not want to assume risk, the military police planner recommends some form of bypass criteria or requests augmentation from higher authority in order to maintain stability. If a credible local enforcement mechanism exists, then the military police planner incorporates and develops transition criteria.

This page is intentionally left blank.

Appendix B

Sample Criminal Intelligence Products

CRIMINT products may range from the simplest form to the most complex. This appendix provides a variety of sample products including the Be on the Look Out (BOLO) alert; HLS and terrorism daily open-source news summaries; wanted posters; and link analysis graphs, charts, and maps.

This appendix is not intended to be an all-inclusive explanation or sample of CRIMINT products. It is intended to show some existing products, provoke thought in creating other CRIMINT products, and get users of such products to consider linkage to other CRIMINT products. When these products, and others like them, are used alone, they assist commanders in making decisions in PIO.

GENERAL

B-1. CRIMINT products may also assist commanders in determining CCIR and COAs. These products may assist ALE personnel in capturing a wanted felon, closing an investigation, or gaining information to assist in an investigation.

B-2. When CRIMINT products are linked to other CRIMINT products or databases, they multiply the opportunities of providing the mechanism with which to capture the wanted person(s) and provide closure to the investigation.

CRIMINAL INTELLIGENCE PRODUCTS

B-3. This appendix will address and show sample copies of the following:

- BOLO alerts.
- Open-source intelligence daily report.
- Wanted posters.
- Link analysis charts, maps, and graphs.
- I&W.

BE ON THE LOOK OUT ALERTS

B-4. BOLO alerts are sent out by ALE and civilian law enforcement agencies. ALE and civilian law enforcement agencies request that if a person recognizes a wanted person that they do not attempt to follow, capture, or conduct a citizens arrest of the individual, but rather that the individual call the contact number and report the sighting. See [Figure B-1](#), page B-2, for a sample BOLO alerts.

OPEN-SOURCE INTELLIGENCE DAILY REPORT

B-5. The next several pages, representing [Figure B-2](#), page B-2, are a sample of an open-source intelligence daily report. This report, provided by North American Aerospace Defense Command (NORAD)/ United States Northern Command (USNORTHCOM), consists of summaries of recent incidents and activities related to HLS and/or terrorism incidents.

For Immediate Release
March 20, 2003 Washington D.C.
FBI National Press Office
Adnan G. El Shukrijumah poster

FBI SEEKING PUBLIC'S ASSISTANCE IN LOCATING INDIVIDUAL
SUSPECTED OF PLANNING TERRORIST ACTIVITIES

The FBI has issued a "Be on the Look Out" (BOLO) alert for Adnan G. El Shukrijumah in connection with possible threats against the United States. In the BOLO alert, the FBI expresses interest in locating and questioning El Shukrijumah, and asks all law enforcement personnel to notify the FBI immediately if he is located. El Shukrijumah's current whereabouts are unknown.

El Shukrijumah is possibly involved with al-Qaeda terrorist activities and, if true, poses a serious threat to U.S. Citizens and interests worldwide.

El Shukrijumah is 27 years old and was born in Saudi Arabia. He is approximately 132 pounds (but may be heavier today), 5'3" to 5'5" tall, has a Mediterranean complexion, black hair, black eyes, and occasionally wears a beard. A photograph of this individual is available on the FBI's website, <<http://www.fbi.gov>>.

El Shukrijumah carries a Guyana passport, but may attempt to enter the U.S. with a Saudi, Canadian, or Trinidad passport as well. El Shukrijumah has gone by the following aliases:

Adnan G. El Shukri Jumah;
Abu Arif;
Ja'far Al-Tayar;
Jaffar Al-Tayyar;
Jafar Tayar;
Jaafar Al-Tayyar

Figure B-1. BOLO Alert

UNCLASSIFIED

Homeland Security/Terrorism Daily Open-Source News Summary

NORAD/USNORTHCOM
Detachment Ft Leavenworth

Use of these articles does not reflect official endorsement. Reproduction for private use or gain is subject to original copyright restrictions.

This report is a compilation of open source information and not evaluated or a final intelligence product. This information is derived from publicly available sources including the Internet and other media. The credibility and reliability of the sources has not been determined.

Figure B-2. Sample of an Open-Source Intelligence Daily Report

2 March 2005

Index

TERRORISM
HOMELAND SECURITY
CYBER NEWS
OTHER ITEMS OF INTEREST

Homeland Security Advisory System Terrorist Threat to the US: **Yemen: Eleven**

Terrorism

Yemen Arrests Several Al Qaeda Suspects¹

Yemeni authorities have arrested a number of suspected al Qaeda members in the Arab state in the last two days, a government newspaper said on Wednesday. The online edition of the weekly, September 26, quoted army sources as saying the arrests were carried out in the capital Sanaa and the port city of Aden, but did not say how many people had been detained. "Those arrested included elements suspected of involvement in terrorist cases or of links to al Qaeda," it quoted a source as saying. "Security forces in Sanaa and Aden are still pursuing some suspects wanted in terrorist and severe criminal cases."

<http://www.metronews.ca/reuters_international.asp?id=59115>

Homeland Security

Where's Iowa's Homeland Security Money Going? ²

Since September Eleventh, the government has spent billions on homeland security. Now some question whether Iowa's getting its fair share of that money. Some people say there's no need to worry about a terrorist attack here in the Midwest. Yet, the Department of Homeland Security has given millions to Iowa. But where's all that money going, and are we getting the right equipment? The government has spent 111 million dollars to keep Iowans safe. <http://www.kcrg.com/article.aspx?art_id=96044&cat_id=123>

State slated to receive \$16 million for homeland security. ³

Rhode Island is getting more than 16 (m) million dollars from the federal government to prepare for a terrorist attack or natural disaster. The funds will go to the state Emergency Management Agency, and are earmarked for specific programs, including a homeland security program. That program is getting more than ten million dollars. <<http://www.wpri.com/Global/story.asp?S=3017902&nav=F2DOWzGL>>

¹ "Yemen Arrests Several Al Qaeda Suspects." Metro News. Access Date: 2 March 2005. Source Date: 2 March 2005. <http://www.metronews.ca/reuters_international.asp?id=59115>

² Geary, Mark. "Where's Iowa's Homeland Security Money Going?" KCRG.com. Access Date: 2 March 2005. Source Date: 1 March 2005. <http://www.kcrg.com/article.aspx?art_id=96044&cat_id=123>

³ "State slated to receive \$16 million for homeland security." WPRI.com. Access Date: 2 March 2005. Source Date: 2 March 2005. <<http://www.wpri.com/Global/story.asp?S=3017902&nav=F2DOWzGL>>

Figure B-2. Sample of an Open-Source Intelligence Daily Report (Continued)

Cyber News

Open-Source Cyber News Summary – Ft. Leavenworth, CIAP-Cyber Threats

NIST releases final security guidelines⁴

A final version of security guidelines designed to protect federal computer systems and the information they hold was released Monday by the National Institute of Standards and Technology. The guidelines will serve as a road map for federal agencies in meeting mandates set by the Federal Information Security Management Act (FISA). Government agencies will be required to have certain security controls, policies and procedures in place. http://news.com.com/NIST+releases+final+security+guidelines/2100-7348_3-5593256.html

Security Firm Warns of Mozilla, Firefox Security Hole⁵

Hackers can grab control of computers by taking advantage of vulnerabilities in both the Mozilla browser suite and the Firefox stand-alone browser, a security intelligence firm said Monday. According to Reston, Va.-based iDefense, Mozilla 1.7.3 and Firefox 1.0 – and likely all earlier versions as well – include a "design error" that lets hackers create a memory heap overflow, which then allow remote code execution and a compromise of the system. Even a failed attempt to exploit this flaw could bring down the browser, added iDefense. <http://www.securitypipeline.com/60404115>

Other Items of Interest

Beirut opposition plans next move⁶

Lebanese opposition groups are deciding whether to take part in talks to form a new government after the previous administration resigned amid protests. President Emile Lahoud should consult MPs before appointing a new prime minister, under the constitution. But some want Mr Lahoud himself to quit, saying he is too close to Syria, which still dominates much of Lebanon. http://news.bbc.co.uk/2/hi/middle_east/4311201.stm

Iran Produces New Armor-Piercing Sniper Guns⁷

(Full Article) Iran has begun to produce heavy machine-guns with armor-piercing bullets, Iranian state television reported today. Iranian Defense Minister Ali Shamkhani said the 12.7-millimeter gun has a range of 2.5 kilometers and is suitable for snipers.

"The United States had protested to a European country about selling the gun [to Iran], while we have already produced it," Shamkhani said. "Today the first consignment of the weapon was delivered. Now our snipers can target the enemy in their armored personnel carriers and

⁴ Kawamoto, Dawn. "NIST releases final security guidelines." CNetNews. Access Date: 2 March 2005. Source Date: 28 February 2005. <http://news.com.com/NIST+releases+final+security+guidelines/2100-7348_3-5593256.html>

⁵ "Security Firm Warns Of Mozilla, Firefox Security Hole." SecurityPipeline.com. Access Date: 2 March 2005. Source Date: 28 February 2005. <<http://www.securitypipeline.com/60404115>>

⁶ "Beirut opposition plans next move." BBC. Access Date: 2 March 2005. Source Date: 2 March 2005. <http://news.bbc.co.uk/2/hi/middle_east/4311201.stm>

⁷ "Iran Produces New Armor-Piercing Sniper Guns." Israel National News. Access Date: 2 March 2005. Source Date: 1 March 2005. <<http://www.israelnationalnews.com/news.php3?id=77700>>

Figure B-2. Sample of an Open-Source Intelligence Daily Report (Continued)

concrete bunkers." The gun weighs 35 pounds and can be mounted on a vehicle. There is widespread concern that the guns will reach the hands of Hizbullah and other terror groups. Iran also produces the Shihab-3 missile, capable of reaching Israel, its own brand of tanks, armored personnel carriers, missiles and even a fighter plane. <<http://www.israelnationalnews.com/news.php3?id=77700>>

China Bids to Restart North Korea Nuclear Talks⁸

A senior Chinese official planned to begin three days of talks in South Korea today as part of efforts to restart stalled six-party negotiations on North Korea's nuclear weapons programmes. Chinese Deputy Foreign Minister Wu Dawei was scheduled to meet his counterpart, Song Min-soon. Wu and Song are top negotiators in the North Korean nuclear dispute. <<http://www.news.scotsman.com/latest.cfm?id=4197426>>

Taiwan Claims China has 706 Missiles⁹

(Full Article) In an appeal to the European Union (EU) not to lift of arm embargo, Taiwanese President Chen Shu-bian has said China had 496 missiles in 2003 and that the amount has increased to 706.

In a teleconference with members of the European Parliament, Chen claimed that China targets Taiwan and it adds 120 middle and short-range missiles every year. He stressed that the Chinese have 173 strategic missiles and 496 tactical missiles along its southeastern coast.

According to the Taiwanese President, if the EU lifts the embargo imposed on the Beijing administration, this will send a wrong message to China. The EU plans to lift the Chinese embargo in the next six months. US President George W. Bush has announced concern over the EU's plan. <<http://www.zaman.com/?bl=hotnews&alt=&trh=20050302&hn=17079>>

⁸ "China Bids to Restart N Korea Nuclear Talks." Scotsman.com. Access Date: 2 March 2005. Source Date: 2 March 2005. <<http://news.scotsman.com/latest.cfm?id=4197426>>

⁹ "Taiwan Claims China has 706 Missiles." Zaman Online. Access Date: 2 March 2005. Source Date: 2 March 2005. <<http://www.zaman.com/?bl=hotnews&alt=&trh=20050302&hn=17079>>

Figure B-2. Sample of an Open-Source Intelligence Daily Report (Continued)

WANTED POSTERS

B-6. Wanted posters bring criminals to justice by putting their faces in the public's view. The posters show the community who is dangerous and keeps the public aware that there are fugitives loose in their community. The picture can be either an artist's sketch or a photograph. An artist's sketch is a rendering of the suspect through the eyes of the witness. The photograph should be as recent as possible. Below the sketch or photograph, there should be a short history of the criminal, including date of birth, sex, height, weight, hair and eye color, scars or marks, occupation, social security number, nationality, place of birth, and all known aliases. Wanted posters are posted by local, state, and federal agencies.

B-7. Posters give a detailed description of the events that occurred during the crime. Posters usually contain a few remarks on what to do when an individual observes the wanted person. If a reward is offered, the poster states how much it is and who is providing it. *Figures B-3 and B-4*, pages B-6 and B-7, represent samples of wanted posters.

LINK ANALYSIS MAPS, CHARTS, AND GRAPHS

B-8. These tools are used to assist in developing crime trends and patterns. They help ALE personnel determine what crimes are taking place where and when. When coupled with the S2's efforts, these tools may link crimes to terrorist-related activity that may impact the operational picture, the IPB, and the CCIR. *Figure B-5*, page B-8, depicts information that these tools may portray.

INDICATIONS AND WARNINGS

B-9. Battalion staff and ALE analysts frequently use I&W in the development of CRIMINT products. *Joint Publication (JP) 3-13* defines I&W as those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to US or allied and/or coalition military; political or economic interests; or US citizens abroad. I&W include forewarning of enemy actions or intentions; the imminence of hostilities; an insurgency; a nuclear or nonnuclear attack on the US, its overseas forces, or allied and/or coalition nations; hostile reactions to US reconnaissance activities; terrorist attacks; and other similar events.

B-10. *FM 2-0* reinforces this definition by stating that I&W come from time-sensitive information and analysis of developments that could involve a threat to US and multinational military forces, US political or economic interests, or US citizens. While the G2 or S2 is primarily responsible for producing I&W intelligence, each element (such as the military police conducting PIO) within every unit contributes to I&W through awareness of the CCIR and by reporting related information.

 WANTED U.S. POSTAL INSPECTION SERVICE	
Osayi Ojo	
	Violations: Credit card fraud. 18 USC 1209(a)(2)
	Case No.: 214-1188830-CID(1)
	NCIC No.: W055879164
	FBI No.: 142754-JAO
	Warrant No.: 02/02/98, District of Massachusetts
	Aliases: David Festus, Travis Ojo, Calvin Johnson, Musa Osayi
	DOB: 11/27/57, Nigeria
Description: Black male, 5'7", 150 lbs., black hair, brown eyes.	
Misc. Info.: None	
TAKE NO ACTION TO APPREHEND THIS PERSON YOURSELF. If located, please call the Northeast Division at (617) 556-4400 or your nearest Postal Inspector in Charge. All information will be kept strictly confidential.	

Figure B-3. Sample of a US Postal Inspection Wanted Poster

Wanted

ARMED AND EXTREMELY DANGEROUS

PHOTO:

NAME: BILL WINTEN

DOB: NOVEMBER 29, 1985

SEX: MALE

HEIGHT: 6' 1"

WEIGHT: 195 POUNDS

HAIR: BROWN

EYES: BROWN

RACE: WHITE

SCARS OR MARKS: BULLET WOUND ON THE LOWER THIGH AND ON THE RIGHT ARM; SCAR ON RIGHT WRIST, SCAR ON THE LEFT THIGH, AND SCAR ON THE LEFT ANKLE. ALSO HAS TRACK MARKS ON HIS RIGHT ARM AND BETWEEN HIS TOES.

OCCUPATION: CONSTRUCTION

SSN USED: 123-45-6789

NATIONALITY: AMERICAN

PLACE OF BIRTH: MIAMI, FLORIDA

ALIAS: BILL JOHNSON; JAMES WILLIAM LONG, JR.

IF YOU HAVE ANY INFORMATION CONCERNING THIS CASE, CONTACT YOUR LOCAL GROCCER.

ANY ADDITIONAL PICTURES:

THE CRIME: UNLAWFUL FLIGHT TO AVOID PROSECUTION – ATTEMPTED MURDER. BILL WINTEN IS BELIEVED TO BE CONNECTED WITH THE ATTEMPTED MURDER OF A STATE TROOPER WHEREIN A .357-CALIBER PISTOL WAS USED.

REWARD: YOUR LOCAL GROCCER IS OFFERING UP TO \$50,000 FOR THE APPREHENSION OF BILL WINTEN.

REMARKS: BILL HAS BEEN KNOWN TO BE ASSOCIATED WITH THE KLU KLUX KLAN AND OTHER RACIST GROUPS.

SOURCES: SARASOTA COUNTY SHERIFFS DEPARTMENT

FBI HOMEPAGE: <<http://www.FBI.gov>>

WRITTEN BY: ROBBY BURNS



Figure B-4. Sample of an FBI Wanted Poster

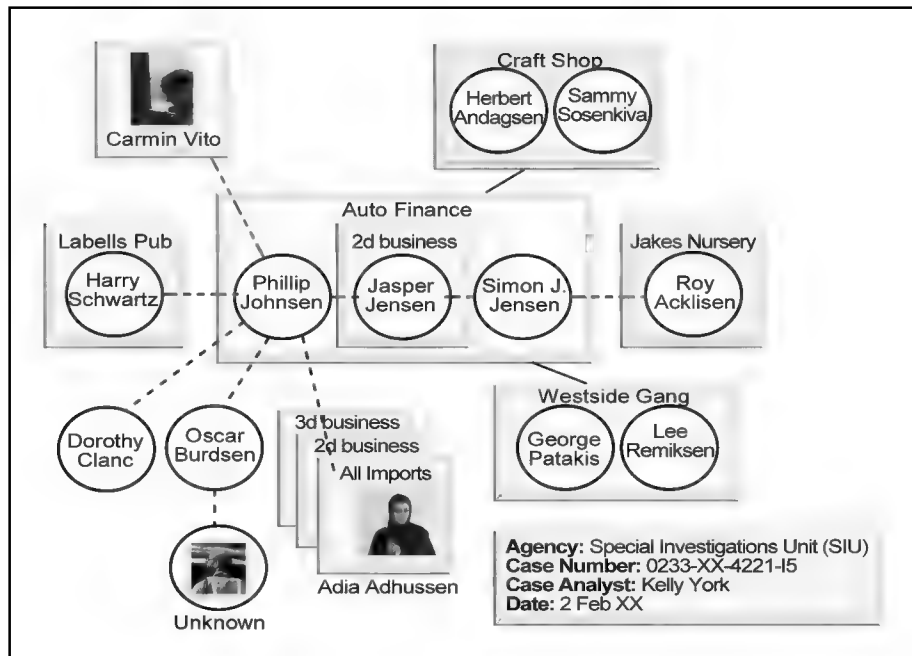


Figure B-5. Link Analysis Chart

Appendix C

Sample Police Intelligence Operations Checklist

The list of questions in *Figure C-1* has been devised to assist managers and operators in PIO. The questions listed in *Figure C-1* are not all-inclusive. Each question listed should be answered yes or no. If any questions are answered no, corrective action must be taken (see *Figure C-1*).

PIO Checklist	Yes	No
Has the SJA been consulted to ensure that there are no legal issues associated with this operation?		
Does the brigade/battalion have an SOP that covers PIO?		
Are all personnel aware of the restrictions placed on the collection of information?		
Were the intelligence process and the IPB process followed during the threat analysis to aid in identifying the local threat?		
Does the threat analysis include—		
• Area geography?		
• Law enforcement resources?		
• Population and cultural factors?		
• Communications capabilities?		
• Possible criminal COAs?		
Have all sources of information for the threat analysis process been identified (for example, MI; CI; and federal, state, and local law enforcement agencies)?		
Have liaison and coordination for information sharing with federal, state, and local law enforcement agencies and the HN (if applicable) been established?		
Has the local threat been identified as an immediate or long-term threat?		
Have other threats been identified (for example, national and international groups that might target the US)?		
Has the threat analysis identified HRP, MEVAs, or HRTs vulnerable to terrorist attack?		
Does the threat assessment include the threat(s) identified in the higher headquarters' threat assessment?		
Has the threat assessment been updated periodically?		
Are reporting procedures established?		
Are all lines of communication established?		
Was corrective action taken for the questions that were answered no?		

Figure C-1. Sample PIO Checklist

This page is intentionally left blank.

Appendix D

Tactical Questioning

FM 2-0 describes tactical questioning. According to this manual, Soldiers develop special levels of situational awareness due to exposure to events occurring in their AO. Soldiers have the opportunity to collect information by observing and interacting with the population and the environment. They can also give useful information to assist the commander in achieving situational understanding. ALE missions often require close contact with the local population.

DEFINING TACTICAL QUESTIONING

D-1. Tactical questioning is a critical element for small unit operations. A more complete operations picture is developed for the commander through tactical questioning, observing the local environment, and interacting with the local population during the conduct of PIO and other missions such as processing EPWs/detainees and handling captured enemy documents and equipment. Soldiers serve as valuable sources of information; they serve as the commander's eyes and ears while—

- Performing traditional offensive or defensive missions.
- Collecting police information.
- Performing a patrol in a stability operation.
- Performing security in operations such as OIF.
- Manning a checkpoint or a roadblock.
- Occupying an OP.
- Escorting convoys.
- Passing through areas in convoys.
- Observing and reporting the environmental elements and activities of the population in the AO.

D-2. Tactical questioning is the expedient, initial questioning of individuals to obtain information of immediate value. When tactical questioning involves interacting with the local population, it is not really questioning; it is more conversational in nature. Tactical questioning can be designed to build rapport with the local population while collecting information and understanding the environment. The Soldier conducts tactical questioning according to the unit's SOP, ROE, and orders for that mission. Small unit leaders must include specific guidance for tactical questioning in the OPORD for appropriate missions. The brigade and battalion S2s and S3s must provide specific guidance in the form of special orders and requests down to company, troop, or battery level to help guide tactical questioning. The information that the Soldier reports as a result of tactical questioning is passed up the chain of command (including the battalion and brigade S2s) and is a vital part of planning and operations. The careful and quick handling of EPWs/detainees and documents by military police may also help the ISR effort.

D-3. Tactical questioning differs from interrogation. Interrogation is defined as a systematic effort to procure information to answer specific collection requirements by using direct and indirect questioning techniques. Interrogation is conducted only by personnel trained to use legal and approved methods of convincing individuals to cooperate.

INTERACTING WITH AND COLLECTING INFORMATION FROM THE LOCAL POPULATION

D-4. Information collection can and should occur at all times in an OE. Collection of combat information consists of becoming familiar with the surrounding environment, to include the people, infrastructure, and terrain. Collection of combat information also includes recognizing change. Like a police officer patrolling in a neighborhood day after day, Soldiers at all ranks and echelons must be able to recognize that something has changed and determine why, if possible. Even if the Soldier cannot determine why something has changed, he should report that there has been a change. This may help MI personnel. Soldiers should train themselves to become constantly aware of conditions concerning—

- Armed elements. Consider the location of factional forces, minefields, and potential threats.
- Homes and buildings. Consider the condition of the roofs, doors, windows, lights, power lines, water system, sanitation system, roads, and bridges.
- Infrastructure. Consider the presence of functioning stores, service stations, and similar establishments. Look for antennas on or near buildings that could be used for communications.
- People. Consider all characteristics of the population. Determine how many people there are; their sexes; their ages; if they are a resident of the area, a displaced person, a refugee, or an evacuee; and their health conditions, their daily clothing, their daily activities, and their leaders.
- Environmental changes. Look for changes in appearance. For example, new locks on buildings, boarded up windows, and previously boarded-up windows now open. Look for anything that indicates a change in the use of a building. Note buildings that have been defaced with graffiti.

D-5. Everyone involved in the collection of combat information must be aware of the IR. All Soldiers who have contact with the local population, routinely travel in the area, or frequently attend meetings with local organizations must know the commander's IR and their responsibility to observe and report.

CONSIDERATING THE ELEMENTS OF COMMUNICATION

D-6. A conversation may be more effective and productive if the elements of communication are considered. Various AOs have different social and regional considerations that affect communications and can affect operations. These may include social taboos, desired behaviors, customs, and courtesies. The staff must include this information in predeployment training at all levels to ensure that Soldiers are properly equipped to interact with the local population. Soldiers must also keep in mind safety considerations and possible dangers associated with their actions. Soldiers must—

- Know the threat level and FP measures in the AO.
- Be knowledgeable of local customs and courtesies.
- Be careful of their body language.
- Approach people in normal surroundings to avoid suspicion.
- Be friendly and polite.
- Remove sunglasses when speaking to people with whom a favorable impression is attempted.
- Know information about the local culture and a few phrases in the local language.
- Understand local customs (for example, male Soldiers not speaking to female civilians, female Soldiers not speaking to male civilians).
- Position weapons in the least intimidating position as possible if security conditions permit.
- Ensure that they do not cluster in such close proximity of each other that they cannot provide cover for one another.
- Ensure that they never lose sight of team members.

ASKING QUESTIONS

D-7. Asking questions is the best way to open and maintain conversation. Try to use open questions that cannot be answered "yes" or "no." An open question is a basic question that usually begins with an interrogative (who, what, where, when, how, or why) and requires a narrative answer. These questions are

brief and simply worded to avoid confusion. For example, "When was the last time an enemy patrol passed through here?" is a better question than, "Have you seen the enemy?" The better question requires a narrative response and requests specific elements of information. Well-crafted, open questions—

- Are broad in nature and serve as an invitation to talk. They require an answer other than "yes" or "no."
- Give the individual answering the questions freedom in his responses. These types of questions do not offer a forced choice such as, "Was the man tall or short?" The answer to that question could be confusing, and it does not allow for responses such as, average or medium height or other descriptive responses.
- Encourage discussion. Let the individual being questioned know that his opinion or observations are of interest.
- Allow the individual to talk while the Soldier listens and observes. The Soldier should look for signs of nervousness or other nonverbal communication.
- Pose no or little threat to the individual. Not all questioning is targeted at information collection. Asking questions about neutral or safe topics can help build rapport with the individual.
- Allow people to become involved. People like to think that their opinion is important. Asking what people think allows them to feel that they are involved.
- Obtain answers that reveal what the individual thinks is important. If relating an experience, people will often start with what is most important to them.
- Create a conversational tone. For example, a simple question about family, work, or hobbies allows an individual to talk freely since the topic is nonthreatening and is one that they know about. These nonpertinent questions can serve as a springboard to topics more closely related to the collection requirement, often without the individual you are talking to realizing that the topic has changed.
- Should be subtle throughout the conversation. Remember to be sociable, but reserved at all times. Rattling off a series of questions and writing down the responses will not gain the trust of the individual that is being addressed.

MAINTAINING THE CONVERSATION

D-8. Some common techniques Soldiers should use to maintain the conversation once it is established are to—

- Avoid using military jargon, especially with civilians.
- Be prepared to discuss personal interests (such as hobbies, books, and travel).
- Be sensitive to your own body language. You must remember to—
 - Smile as long as it is appropriate.
 - Avoid sitting with your arms crossed.
 - Avoid showing the bottoms of your feet in an Arabic culture.
 - Keep hands away from your mouth.
 - Lean forward and nod.
 - Make frequent eye contact (if culturally appropriate).
- Use the individual's name, position title, rank and/or other verbal expressions of respect.
- Avoid judging the individual by age, gender, or appearance.
- Keep body posture relaxed, but alert.
- Remember that an individual's favorite topic is himself or herself.
- Use humor carefully. Some cultures consider excessive humor to be offensive or a sign of deceit.
- Understand the significance of holidays, religious days, or religious times of the day or the week.
- Have a second individual listen to the conversation and later compare what was heard for accuracy.

Note: Comparing observations regarding the individual's eyes (that can indicate deception) and hands can provide insight to the individual's truthfulness. Hand gestures can indicate what the individual was doing. For instance, twisting of hands may represent fabrication of information or nervousness.

Note: Although not a factor in maintaining the conversation, the individual asking the questions must be aware that he may be observed by another individual. The questioner should establish countersurveillance when conducting questioning of an individual to determine whether another individual is observing his operation or the individual being questioned. It should be noted whether the observer approached the individual who was just questioned. The observer's activity may represent that information is collected about the questioner or that the individual just questioned was warned not to speak with the questioner again.

QUESTIONING NONCOMBATANTS

D-9. When conducting tactical questioning of noncombatants, it is imperative that the provisions of the *Geneva Conventions* and *FM 27-10* be followed at all times. Detainees are not to be mistreated in any way. Do not—

- Attempt to force or scare information from noncombatants.
- Attempt to recruit or task someone to go seek out information.
- Give or offer compensation in return for information.
- Ask questions of noncombatants in an area where the questioning puts the noncombatant in danger. Be discreet, but not so discreet to attract attention.
- Ask questions that make the unit's mission or IR obvious.
- Take notes in front of the individual after asking the question.
- Ask leading questions.

Note: Leading questions are questions that typically require a "yes" or "no" answer rather than a narrative answer. Leading questions allow the individual to answer with a response that he thinks is desired and not necessarily the facts.

- Ask negative questions.

Note: Negative questions are questions that contain a negative word in the question itself, such as "Didn't you go to the warehouse?" Instead, ask "Did you go to the warehouse?"

- Ask compound questions.

Note: Compound questions consist of two questions asked at the same time; for example, "Where were you going after work and who were you meeting there?" The individual may only answer one of the questions or may become confused by multiple questions asked at the same time.

- Ask vague questions.

Note: Vague questions do not have enough information for the individual to understand exactly what is being asked. His answers may be incomplete, general, and nonspecific and create doubt.

Appendix E

Questions to Ask Detainees

The following list of questions has been devised to assist individuals in questioning detainees. The list is not all inclusive. Detainees should answer each question as fully as possible, while proper and humane treatment of each detainee is afforded. The questions are—

- What is your name (including any aliases)?

Note: Have the detainee legibly write his name.

- What is your date of birth?
- What is your place of birth?
- What is your address?
- What is your height and weight?
- What gang, clan, and/or tribe are you affiliated with?
- What is your hair color?
- What is your eye color?
- What scars, tattoos, or other identifying marks do you have?

Note: Take photographs if possible.

- Are you married, single, or divorced?
- What is your religious preference?
- What is the current location of your immediate family (spouse and children) and how many of them are there?
- What is your next of kin's phone number and address?
- Do you have any medical conditions (such as allergies to medications) or diseases (such as tuberculosis, hepatitis, or Acquired Immune Deficiency Syndrome)?
- What is your blood type?
- Do you have any friends and associates you wish to have contacted while you are detained?
- Do you have any other conditions? For example, do you have any psychological disorders, take any medication, wear dentures, wear eye glasses or contacts, or have prosthetic limbs.
- Do you have a passport or Voluntary Intermodal Sealift Agreement (VISA)?
- Do you have transportation? If yes, where is it?
- Are there any warrants out for you?

This page is intentionally left blank.

Appendix F

Debriefings and/or After-Action Reviews

This appendix is designed to assist the individuals responsible for conducting PIO debriefings and/or AARs. The areas addressed are generic in nature and are not all-inclusive.

MILITARY (FACTION) ACTIVITIES

F-1. Debriefings and/or AARs are meetings from which to collect battle order information. This information includes—

- Unit identification, size, and disposition.
- Personnel strength.
- Personnel activities.
- Equipment and its condition.
- Weapons, their conditions, and their states of preparedness.
- Special weapons, their quantities, and their deployment.
- Vehicles and their conditions.
- Petroleum, oils, and lubricants supply levels.
- Available transportation.

F-2. After identifying the battle order information, it should be determined if this information represents a change from the norm. The reaction (if any) to the presence of a US or multinational force patrol should also be noted.

CIVILIAN ACTIVITIES (LOCAL POPULATION)

F-3. The presence and activities of civilians can often provide valuable information relating to the activities of military and other operatives in an area. Details that seem insignificant, such as the doors to residences being closed when they are usually open, may indicate that something is about to happen. The closed doors may indicate that civilians have been alerted to take cover. Debriefing and/or AAR questions regarding civilian activities should include the following:

- What is the ethnic makeup of the population?
- Are disparate ethnic groups congregating together?
- Are the usual civilian activities occurring?
- Are there unusually large gatherings of people present?
- Are normal gatherings missing or are they significantly smaller than usual?
- Is there graffiti present and what message does it convey?

F-4. After identifying the above information, it should be determined if this information represents a change from the norm. The reaction (if any) to the presence of a US or multinational force patrol should also be noted.

INFRASTRUCTURE CONDITIONS OR STATUS

F-5. Infrastructure is another significant area in which critical information can be gathered. Debriefing and/or AAR questions regarding infrastructure conditions or status should include the following:

- Are the roads passable?
- Are the structures usable?
- Are utilities (water, electric, and sewer) functional and adequate?
- Are radio stations broadcasting any anti- or pro-US statements?
- Are schools, hospitals, and post offices open?
- Are NGOs operating in the area? If so, what are they doing?
- Is there any interference with NGO activity? If so, by whom?
- Are there any food shortages? If so, what are they?

F-6. After identifying the above information, it should be determined if any of the information represents a change from the norm. The reaction (if any) to the presence of a US or multinational force patrol should also be noted.

Appendix G

Sources

Sources are valuable law enforcement tools. Sources bring risks to the agency and themselves. The reliability of sources and the information disclosed to the source should be considered. As a rule, ALE personnel should disclose the least amount of information concerning the law enforcement operation with the source. The disclosure of too much information to a source could jeopardize the investigation and the safety and identification of ALE officers. Sources may be collecting as much information on law enforcement as law enforcement is attempting to collect on the criminals. This appendix will address open and nonopen sources and covert and overt sources. Sources are the mainstay of law enforcement personnel in their effort to gather police information.

OPEN AND NONOPEN SOURCES

G-1. Open and nonopen sources, while appearing cut and dry on the surface, often entail much more discriminating viewpoints. Before acting on information received from open and nonopen sources, the information must be verified. The decision to maintain a nonopen source as nonopen can be complex. If the source's status is changed to open, it may lead to compromising the source, losing possible future police information and compromising the investigation. Open and nonopen sources are comprised of HUMINT, signal intelligence, and any other media available to the general public.

OPEN SOURCES

G-2. Open sources, as suggested by their name, are open to the public and are easily accessible by anyone. Open sources may be commanders, individuals in positions of responsibility or authority, or anyone that can provide information of significant value.

NONOPEN SOURCES

G-3. Nonopen sources are not as readily available to the public as open sources. Generally, if a nonopen source is used, there is a requirement to register and pay a fee.

Note: The US Army and CID use specific criteria to further identify types of nonopen sources. Those criteria are beyond the scope of this manual.

OVERT SOURCES

G-4. Overt collection efforts are simply information-gathering efforts where concealment of the effort is not a priority. While information collection efforts should always be considered sensitive and involve only those with a need to know or a need to be involved, it is in no way secret. Overt sources include—

- Newspapers, magazines, periodicals, and the media.
- Service records, leases, medical records, and job applications.
- Open Internet sources.
- Interviews and interrogations.

COVERT SOURCES

G-5. Covert collection sources and information gathering is designed to keep the collection effort secret. It often involves the use of registered sources or undercover personnel. Additionally, surveillance provides another covert collection method to obtain information.

G-6. Surveillance can be manned or unmanned and involves the use of multiple pieces of equipment. Surveillance may be as simplistic as a stakeout or as extreme as using satellite imagery. While most surveillance falls somewhere in the middle, photographic evidence should be obtained to document evidence, as needed. The advancement of video/photography capabilities should be considered.

G-7. Wire authority (recordings) should be obtained according to agency policies and existing laws. Current federal law concerning the recording of personal conversations requires that only one party consent to recording the conversation. State laws often vary and may require two-party consent. It is the responsibility of the law enforcement officer recording the conversation to familiarize himself with local and state laws concerning wire authority. The court (state or federal) in which the case will be presented determines which legal restrictions apply. Wire authority does not require a warrant signed by a judge or federal magistrate. Unlike wiretaps and other covert listening devices, wire authority to record conversations is usually limited between sources or undercover agents and a specific individual. Wiretaps/covert listening devices usually require a warrant or court order signed by a federal judge or federal magistrate. The physical location, specific individuals, and suspected information to be gained are usually outlined in an affidavit and presented before a federal judge or federal magistrate. Additionally, the warrant usually outlines the restrictions concerning the type of equipment to be used and identifies the time frame of the authority under which the recording can be used.

G-8. Undercover operatives are excellent sources for covert information and intelligence gathering. The use of undercover operatives should be considered when there is a need for long-term intelligence. There are drawbacks associated with using undercover operatives. These drawbacks can include long establishment time, high costs, and intensive manpower requirements. The advantages of using undercover operatives in an investigation can be firsthand knowledge of the information/intelligence by a law enforcement officer. Undercover operatives are the preferred covert sources because they provide credibility during the prosecution of a suspect.

Glossary

Acronym/Term	Definition
AAR	after-action review
ACE	analysis control element
ACERT	Army Computer Emergency Response Team
ACI2	Army criminal investigative information system
ACIC	Army Counterintelligence Center
AI	area of interest
ALE	Army law enforcement
AO	area of operation
AOR	area of responsibility
AR	Army regulation
ARNG	Army National Guard
AS	area security
AT	antiterrorism
ATO	anti-terrorism officer
ATOIC	Antiterrorism Operations Intelligence Cell
ATTN	attention
BATF	Bureau of Alcohol, Tobacco, and Firearms
bde	brigade
BN	battalion
BOLO	Be on the Look Out
C2	command and control
CA	civil affairs
CALL	Center for Army Lessons Learned
CASCOPE	civil areas, structures, capabilities, organizations, people, and events
CBRN	chemical, biological, radiological, and nuclear
CBRNE	chemical, biological, radiological, nuclear, and high-yield explosives
CCIR	commander's critical information requirement
CDR	commander
CEO	Chief Executive Officer
CI	counterintelligence
CIA	Central Intelligence Agency
CIASE	Criminal Intelligence Analytical Support Element
CID	Criminal Investigation Division Command
CIF	central issue facility
CIVPOL	civilian police

COA	course of action
CONUS	continental United States
COE	contemporary operational environment
COPS	Centralized Operator's Police Suite
CRIMINT	criminal intelligence
DA	Department of the Army
DCIS	Defense Criminal Investigative Services
DEA	Drug Enforcement Administration
DES	director of emergency services
DIA	Defense Intelligence Agency
DOD	Department of Defense
DISC4	director of information systems for command, control, communications, and computers
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DOIM	director of information management
DP	decision point
DPTM	Director of Plans, Training, and Mobilization
EBO	effects-based operations
ECOA	enemy course of action
EEFI	essential elements of friendly information
EEI	essential elements of information
EO	executive order
EOC	Emergency Operations Center
EOD	explosive ordnance disposal
EPW	enemy prisoner of war
EU	European Union
FBI	Federal Bureau of Investigations
FFIR	friendly force information requirements
FISA	Federal Information Security Management Act
FM	field manual
FOIA	Freedom of Information Act
FP	force protection
FPCON	force protection condition
Ft	Fort
G2	assistant chief of staff, intelligence section
G3	assistant chief of staff, operations and plans
G5	assistant chief of staff, civil affairs
GS	general support
HLS	Homeland Security
HN	host nation

HPT	high-payoff targets
HQ	headquarters
HQDA	Headquarters, Department of the Army
HR	hour
HRP	high-risk person
HRT	high-risk targets
HUMINT	human intelligence
I/R	internment/resettlement
IMA	Installation Management Agency
INSCOM	Intelligence and Security Command
intel	intelligence
IO	information operations
IPB	intelligence preparation of the battlefield
IR	information requirements
ISR	intelligence, surveillance, and reconnaissance
I&W	indications and warnings
J2	joint intelligence section
JP	Joint Publication
JR	Junior
JWICS	Joint Worldwide Intelligence Communications System
LO	law and order
lbs.	pounds
LES	law enforcement sensitive
LIWA	Land Information Warfare Activity
m	million
MACOM	major army command
MANSCEN	maneuver support center
MDMP	military decision-making process
MEDDAC	Medical Department Activity
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations
MEVA	mission-essential vulnerability area
MI	military intelligence
MMS	maneuver and mobility support
MO	modus operandi
MOA	memorandum of agreement
MOU	memorandum of understanding
MP	military police
MSC	major supporting command

MSR	main supply route
NAI	named area of interest
NCIC	National Crime Information Center
NCOES	Noncommissioned Officer Education System
NG	National Guard
NGO	nongovernmental organization
NIPERNET	nonsecure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NO	number
NORAD	North American Aerospace Defense
NSA	National Security Agency
OAKOC	observation and fields of fire, avenues of approach, key terrain, obstacles and movement, and cover and concealment
OCONUS	outside the continental United States
ODCSOPS	Office of the Deputy Chief of Staff for Operations and Plans
OE	operational environment
OEF	Operation Enduring Freedom
OES	Officer Education System
OIF	Operation Iraqi Freedom
OP	observation post
OPLAN	operation plan
OPORD	operation order
OPS	operations
OPSEC	operational security
OPTEMPO	operating tempo
PAO	public affairs office
PDP	patrol distribution plan
PIO	police intelligence operations
PIR	priority intelligence requirements
PM	provost marshal
PMO	Provost Marshal Office
POLICE	police and prison structures, organized crime, legal systems, investigations, crime-conducive conditions, and enforcement mechanisms and gaps
PSVAs	personal security vulnerability assessments
PSYOP	psychological operation
RAM	random antiterrorism measures
REL	release
RFI	request for information
ROE	rules of engagement

R&S	reconnaissance and surveillance
S1	adjutant
S2	intelligence staff officer (US Army)
S3	operations staff officer
S5	Civil Affairs Officer (US Army)
SAC	special agent in charge
SALUTE	size, activity, location, unit, time, and equipment
SECDEF	Secretary of Defense
SGT	sergeant
SIPERNET	secure Internet Protocol Router Network
SIPRNET	secret Internet Protocol Network
SITREP	situation report
SIU	Special Investigations Unit
SJA	Staff Judge Advocate
SO	security officer
SOFA	status of forces agreement
SOP	standing operating procedure
SSN	social security number
TALON	threats and local observation notices
TCP	traffic control point
THT	tactical human intelligence team
TRADOC	Training and Doctrine Command
UN	United Nations
UNCIVPOL	United Nations civilian police
UO	urban operations
US	United States
USACIDC	United States Army Criminal Investigations Command
USAMPS	United States Army Military Police School
USC	United States Code
USNORTHCOM	United States Northern Command
Va.	Virginia (the state of)
VISA	Voluntary Intermodal Sealift Agreement
WFF	warfighting function
XO	executive officer

This page is intentionally left blank.

References

SOURCES USED

AR 25-55. *The Department of the Army Freedom of Information Act Program*. 1 November 1997.

AR 195-1. *Army Criminal Investigation Program*. 12 August 1974.

AR 195-2. *Criminal Investigation Activities*. 30 October 1985.

AR 381-10. *US Army Intelligence Activities*. 22 November 2005.

AR 381-12. *Subversion and Espionage Directed Against the US Army (SAEDA)*. 15 January 1993.

AR 381-20. *The Army Counterintelligence Program*. 15 November 1993.

AR 525-13. *Antiterrorism*. 4 January 2002.

CID Regulation 195-1. *Criminal Investigation Operational Procedures*. 15 June 2004.

DA Form 2804. *Crime Records Data Reference*.

DODD 2000.12. *DOD Antiterrorism (AT) Program*. 18 August 2003.

DODI 2000.16. *DOD Antiterrorism Standards*. 14 June 2001.

EO 12333. *United States Intelligence Activities*. 4 December 1981.

FM 1-02. *Operational Terms and Graphics*. 21 September 2004.

FM 2-0. *Intelligence*. 17 May 2004.

FM 3-0. *Operations*. 14 June 2001.

FM 3-19.4. *Military Police Leaders' Handbook*. 4 March 2002.

FM 3-90. *Tactics*. 4 July 2001.

FM 5-0. *Army Planning and Orders Production*. 20 January 2005.

FM 7-15. *The Army Universal Task List*. 31 August 2003.

FM 27-10. *The Law of Land Warfare*. 18 July 1956.

FM 34-2. *Collection Management and Synchronization Planning*. 8 March 1994.

Geneva Conventions. 12 August 1949

JP 3-13. *Joint Doctrine for Information Operations*. 9 October 1998.

USA Patriot Act, Uniting and Strengthening America By Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. 24 October 2001.

USC, Title 18, Crimes and Criminal Procedure; Part I, Crimes; Chapter 121, Stored Wire and Electronic Communications and Transactional Records Access; Section 2703, required disclosure of customer communications or records.

DOCUMENTS NEEDED

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

READINGS RECOMMENDED

AR 25-400-2. *The Army Records Information Management System (ARIMS)*. 15 November 2004.

AR 190-6. *Obtaining Information From Financial Institutions*. 9 February 2006.

AR 190-27. *Army Participation in Criminal Justice Information Systems, Federal Bureau of Investigation*. 8 November 2005.

AR 190-40. *Serious Incident Report*. 9 February 2006.

AR 190-45. *Law Enforcement Reporting*. 23 February 2006.

References

- AR 380-13. *Acquisition and Storage of Information Concerning Nonaffiliated Persons and Organizations*. 13 September 1974.
- DODD 5200.27. *Acquisition of Information Concerning Persons and Organizations not Affiliated With the Department of Defense*. 7 January 1980.
- DODD 5525.5. *DOD Cooperation With Civilian Law Enforcement Officials*. 15 January 1986.
- FM 34-130. *Intelligence Preparation of the Battlefield*. 8 July 1994.
- USC, Title 22, *Foreign Relations and Intercourse; Chapter 32, Foreign Assistance; Subchapter III, General and Administrative Provisions; Part III Miscellaneous Provisions; Development Assistance Authorizations; Section 2420, Police Training Prohibition*.

Index

- ACIC, 2-5
- ALE, 1-1, 1-7, 2-1, 3-1, 7-7
 - BOLO alerts, B-1
 - Patriot Act, 2-8
 - policy, 1-8
 - sources, G-1
- antiterrorism (AT). *See* AT.
- Antiterrorism Operations Intelligence Cell (ATOIC). *See* ATOIC.
- Army Counterintelligence Center (ACIC). *See* ACIC.
- AT, 1-8, 2-5, 2-6, 2-7, 7-4, 7-5
 - operations, 1-8
- ATOIC, 2-5
- Be on the Look Out (BOLO). *See* BOLO
- BOLO, B-1
- C2, 2-5
- CA, 3-6, 5-2, 5-4
- CCIR, 1-6, 3-1, 4-2
- civil affairs (CA). *See* CA.
- command and control (C2). *See* C2.
- commander's critical information requirements (CCIR). *See* CCIR.
- criminal intelligence (CRIMINT). *See* CRIMINT.
- CRIMINT, 1-1, 1-7, 2-3, 2-6, 3-1, 4-1, 6-1, 7-6, B-1
 - process, 4-1
 - products, B-1
- databases, 4-8
- EOCA, 1-4
- emergency operations center (EOC). *See* EOC.
- enemy course of action (EOCA). *See* EOCA.
- EOC, 3-9
- FBI, 2-1, 4-8, 6-2, 7-2
- Federal Bureau of Investigations (FBI). *See* FBI.
- force protection (FP). *See* FP.
- force protection condition (FPCON). *See* FPCON
- FP, 1-1, 3-5, 5-1, 6-1, 7-4
 - intelligence support, 1-4
 - programs, 1-1
- FPCON, 2-6
- HN, 1-3, 3-7, 5-1, 5-3, 7-2
- host nation (HN). *See* HN.
- Human Intelligence (HUMINT). *See* HUMINT.
- HUMINT, 1-7, G-1
- I/R, 1-7
- IMA, 6-1, 6-2
 - responsibilities, 6-1
- information collection process, 3-7
- information operations (IO). *See* IO.
- information requirements (IR). *See* IR.
- Installation Management Agency (IMA). *See* IMA.
- intelligence preparation of the battlefield (IPB). *See* IPB.
- internment/resettlement (I/R). *See* I/R.
- IO, 2-5, 3-7
- IPB, 1-1, 2-7, 4-1, 5-3
 - performing, 1-3
- IR, 1-6, D-2
- major army command (MACOM). *See* MACOM.
- maneuver and mobility support (MMS). *See* MMS.
- MDMP, 1-4, 3-1, A-1, A-2
- METT-TC, 1-1, A-4
- MEVA, 3-4, 4-3
- MI, 1-1, 2-4
- military decision-making process (MDMP). *See* MDMP.
- military intelligence (MI). *See* MI.
- mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC). *See* METT-TC.
- mission-essential vulnerability area (MEVA). *See* MEVA.
- MMS, 1-7
- NAI, 3-4, 3-6, 3-10, 4-3, 6-4
- named area of interest (NAI). *See* NAI.
- OE, 1-2, 3-7, 5-1, 7-1, D-2
- operational environment (OE). *See* OE.
- Patriot Act*, 2-7
- personal security vulnerability assessment (PSVA), 2-5
- PIO, 1-1, 1-7, 7-2, A-4
 - application, 1-7
 - authority, 6-1
 - development, 3-1
 - forums, 7-4
 - managing, 6-2
 - network, 1-6, 7-1
 - roles, 1-2
- PIR, 1-2, 2-6
- POLICE, 1-4, 5-2, A-4
- police and prison structures, organized crime, legal systems, investigations, crime-conducive conditions, and enforcement mechanisms and gaps (POLICE). *See* POLICE.
- police information collection process, 4-2, 6-4
 - assessing, 3-8
 - collecting and recording, 3-8
 - disseminating, 3-8
 - evaluation and feedback, 3-8
 - observing, 3-8
 - planning, 3-8
- police intelligence operations (PIO). *See* PIO.
- priority intelligence requirements (PIR). *See* PIR.
- PSVA, 2-5
- psychological operation (PSYOP). *See* PSYOP.
- PSYOP, 3-6
- R&S, 3-6, 3-10, 5-4, 5-5
- reconnaissance and surveillance (R&S). *See* R&S.
- reporting procedures, 3-8
- ROE, 3-4
- Rules of engagement (ROE). *See* ROE.

SAC, 4-1

special agent in charge (SAC).

See SAC.

urban threats, 5-1

insurgents, 5-1

other threats, 5-2

warfighting function (WFF).

See WFF.

WFF, 1-2

tasks, 1-2

FM 3-19.50
21 July 2006

By Order of the Secretary of the Army:

PETER J. SCHOOMAKER
General, United States Army
Chief of Staff

Official:



JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army
0618101

DISTRIBUTION:

Active Army, ARNG, and United States Army Reserve. To be distributed in accordance with the initial distribution number (IDN) 115970, requirements for *FM 3-19.50*.

This page is intentionally left blank.

